

Peter Julius Waldert

Secure Classification as a Service

BACHELOR'S THESIS

Bachelor's degree programmes:
Physics and Information & Computer Engineering

Supervisors

Dipl.-Ing. Roman Walch

Dipl.-Ing. Daniel Kales

Institute of Applied Information Processing and Communications
Graz University of Technology

Graz, March 2022

Abstract

Abstract of your thesis (at most one page)

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Keywords: FHE, classification, neural network

Technologies: Microsoft SEAL (C++, nodejs), Tensorflow Keras, Numpy, xtensor, Docker, msgpack, React, Materialize, Nginx

Languages: C++, Python, JavaScript

Contents

1	Introduction	4
2	Background	5
2.1	Basics of Fully Homomorphic Encryption	5
2.1.1	Packing	5
2.1.2	HE using RSA	5
2.1.3	Learning with Errors (LWE)	5
2.1.4	Ring-LWE	5
2.1.5	The BFV scheme	6
2.1.6	The CKKS scheme	6
2.2	Machine Learning	6
2.2.1	Linear Regression?	6
2.2.2	Gradient Descent?	6
2.2.3	The Backpropagation Algorithm	6
2.2.4	Multi-Layered Neural Networks	6
2.3	Post-Quantum Security	6
2.4	Demo	6
2.5	Notation and Acronyms	7
2.6	Citations	8
3	Implementation	10
3.1	Chosen Software Architecture	10
3.2	The MNIST dataset	10
3.3	Matrix-Vector Multiplication	10
3.3.1	Adapting to non-square matrices	10
3.4	Polynomial Evaluation	11
3.5	Transparent Ciphertext	11
4	Results	13
4.1	Performance / Runtime Benchmarks	13
4.2	Communication Overhead	13
4.3	Accuracy	13
5	Conclusion	14
	Notation	15
	Acronyms	16
	Bibliography	17

Chapter 1

Introduction

Goal:

Chapter 2

Background

2.1 Basics of Fully Homomorphic Encryption

Homomorphic Encryption (HE) makes it possible to operate on data without knowing it. One can distinguish three flavors of it, Partial-, Semi- and Fully Homomorphic Encryption (FHE).

- Brakerski/Fan-Vercauteren (BFV) scheme for integer arithmetic
- Brakerski-Gentry-Vaikuntanathan (BGV) scheme for integer arithmetic
- Cheon-Kim-Kim-Song (CKKS) scheme for real-number arithmetic
- Ducas-Micciancio (FHEW) and Chillotti-Gama-Georgieva-Izabachene (TFHE) schemes for Boolean circuit evaluation

2.1.1 Packing

FFT in CKKS! Polynom -> Vektor mit einer FFT Vektor -> Polynom mit einer IFFT

2.1.2 HE using RSA

With unpadded RSA, some arithmetic can be performed on the ciphertext - looking at the encrypted ciphertext $\mathcal{E}(m_1) = (m_1)^r \mod n$ of the message m_1 and m_2 respectively, the following holds:

$$\mathcal{E}(m_1) \cdot \mathcal{E}(m_2) = (m_1)^r (m_2)^r \mod n \quad (2.1)$$

$$= (m_1 m_2)^r \mod n \quad (2.2)$$

$$= \mathcal{E}(m_1 \cdot m_2) \quad (2.3)$$

The encryption therefore partially fulfills the properties of ring homomorphism, which in general is defined as follows:

2.1.1 Definition (Ring Homomorphism)

Given two rings $(R, +, \cdot)$ and (S, \oplus, \otimes) , we call a mapping $\varphi : R \rightarrow S$ a ring homomorphism when it satisfies the following conditions:

$$\forall a, b \in R : \varphi(a + b) = \varphi(a) \oplus \varphi(b) \wedge \varphi(a \cdot b) = \varphi(a) \otimes \varphi(b)$$

2.1.3 Learning with Errors (LWE)

2.1.4 Ring-LWE

Learning with Errors on Rings (RLWE)

how to get from LWE to RLWE

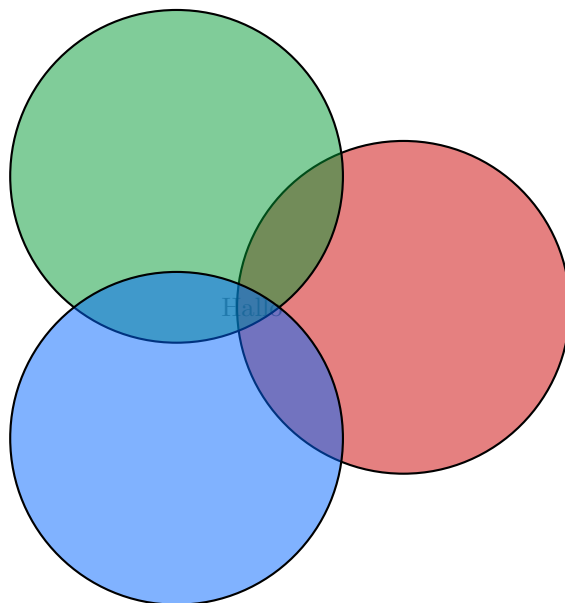


Figure 2.1: Ah yes the caption

2.1.5 The BFV scheme

2.1.6 The CKKS scheme

The CKKS scheme allows us to perform approximate arithmetic on floating point numbers.

2.2 Machine Learning

As Shafi Goldwasser puts it, 'Machine Learning is somewhere in the intersection of Artificial Intelligence, Statistics and Theoretical Computer Science' [Goldwasser 2018](#).

2.2.1 Linear Regression?

2.2.2 Gradient Descent?

2.2.3 The Backpropagation Algorithm

2.2.4 Multi-Layered Neural Networks

Matrix -> Activation Function

- Matrix Multiplication (Dense Layer)
- Convolutional Layer
- Sigmoid Activation
- Max Pooling

2.3 Post-Quantum Security

2.4 Demo

In this chapter, we provide some usage examples for glossaries and acronym lists with `glossaries` ([section 2.5](#)), bibliography and citations with `biblatex` ([section 2.6](#)), and more.

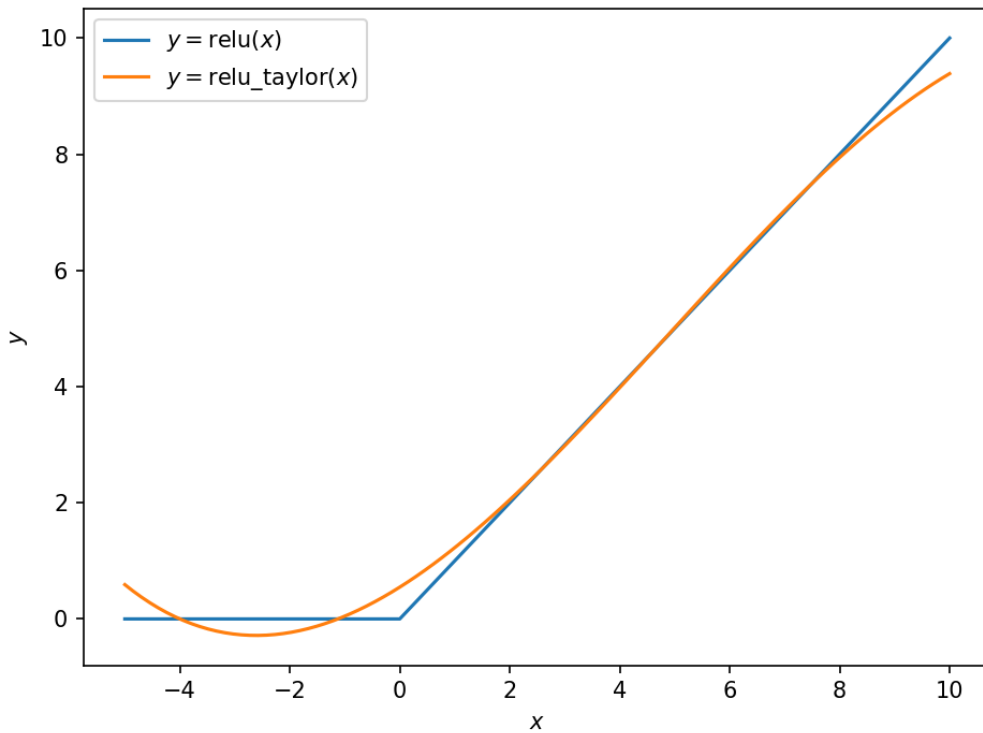


Figure 2.2: Comparison of the Relu activation function vs. its Taylor expansion

2.5 Notation and Acronyms

Symbols and acronyms are defined in the preamble, after loading the `glossaries` package, and used as follows.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetur adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetur.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

In this chapter, we introduce the necessary background on the [Advanced Encryption Standard \(AES\)](#). We denote binary exclusive-or by \oplus .

2.6 Citations

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetur adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetur.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

This is an example of how to specify and cite a book [Daemen and Rijmen 2002](#), a journal article [Shannon 1949](#). [AES](#) is a block cipher defined by [Daemen and Rijmen \(2002\)](#).

Chapter 3

Implementation

3.1 Chosen Software Architecture

In the given setting, the most accessible frontend is commonly a JavaScript web application.

To still make the classification run as quickly and efficiently as possible, a C++ binary runs in the backend providing an HTTP API to the frontend application. In order to allow for more flexibility of the HTTP server, the initial approach was to pipe requests through a dedicated web application framework with database access that would allow, for instance, user management next to the basic classification. However, the resulting communication and computation overhead, even when running with very efficient protocols such as ZeroMQ, was too high.

Extending the accessibility argument to reproducibility, Docker is a very solid choice (Nüst et al. 2020). To run the attached demo project, simply execute

```
1  docker-compose build
2  docker-compose up
```

in the 'code' folder and point your browser to <https://localhost>.

3.2 The MNIST dataset

The MNIST dataset (LeCun and Cortes 1998) contains X train and Y test images with corresponding labels. In order to stick to the traditional feedforward technique with data represented in vector format, therefore it is common to reshape data from (28, 28) images (represented as grayscale values in a matrix) into a 784 element vector.

3.3 Matrix-Vector Multiplication

The dot product that is required as part of the neural network evaluation process needs to be implemented on SEAL ciphertexts as well.

There are multiple methods to achieve a syntactically correct dot product (matrix-vector multiplication) as described by Juvekar, Vaikuntanathan and Chandrakasan (2018) for square matrices.

1. Naive
2. Diagonal
3. Hybrid

3.3.1 Adapting to non-square matrices

The weight matrices in the given classification setting are by no means square, on the contrary their output dimension tends to be much lower than the input dimension as the goal is to reduce it from $28^2 = 784$ to 10 overall.

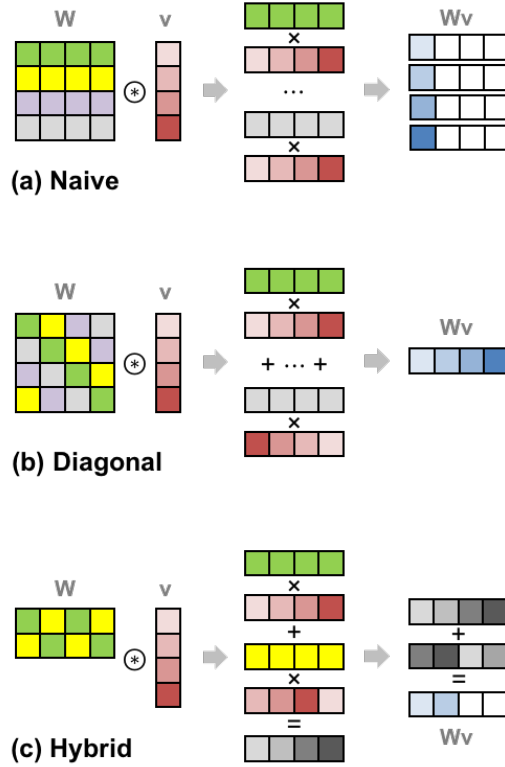


Figure 3.1: Different techniques to compute a dot product between a matrix and a vector, each having their up- and downsides.

However, that also means one cannot directly apply the diagonal method as described in the proceedings above. This 'flaw' can be mitigated by a simple zero-padding approach in order to make the matrix square, filling in zeros until the lower dimension reaches the higher one.

3.4 Polynomial Evaluation

From the implementation perspective, there are three properties to watch out for when working with SEAL ciphertexts:

1. Scale (retrieved using `x.scale()`)

Scale has nothing to do with noise. "Scale out of bounds" can appear even if noise is extremely low. Although repeated multiplication of a ciphertext by a plaintext will slowly increase the noise, it is not the reason why you see "scale out of bounds". "Scale out of bounds" error specifically means that the scale of a ciphertext or plaintext is larger than the product of all elements in `coeff_modulus`. If you perform multiplications without rescaling, you can quickly see this error. The more rescaling you perform, the less elements will be left in `coeff_modulus`. Even if you managed to have the same scale in a ciphertext after every multiplication and rescale, eventually the `coeff_modulus` can be too small to accommodate another multiplication.

2. Encryption Parameters (retrieved using `x.parms_id()`)
3. Ciphertext Size (retrieved using `x.size()`)

3.5 Transparent Ciphertext

The problem is that you are subtracting a ciphertext from itself. This kind of operation results in a ciphertext that is identically zero; this is called a transparent ciphertext. Such a transparent ciphertext is not considered to be valid because the ciphertext reveals its underlying plaintext to anyone who sees it, even if they don't have the secret key. By default SEAL throws an exception

when such a situation is encountered to protect you from a problem you may not have noticed. If you truly know what you are doing and want to enable the creation of transparent ciphertexts, you can configure SEAL [...]. ([Laine 2020](#))

'transparent ciphertexts (a.k.a. ciphertexts whose second polynomial is zero) are malformed and do not need the secret key to decrypt'

Chapter 4

Results

4.1 Performance / Runtime Benchmarks

4.2 Communication Overhead

4.3 Accuracy

Chapter 5

Conclusion

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Notation

\oplus exclusive-or (XOR)

8

Acronyms

AES	Advanced Encryption Standard	8, 9
FHE	Fully Homomorphic Encryption	5
HE	Homomorphic Encryption	5

Bibliography

- Daemen, Joan and Vincent Rijmen (2002). *The Design of Rijndael: AES – The Advanced Encryption Standard*. Information Security and Cryptography. Springer. ISBN: 3-540-42580-2. DOI: [10.1007/978-3-662-04722-4](https://doi.org/10.1007/978-3-662-04722-4).
- Goldwasser, Shafi (2018). ‘From Idea to Impact, the Crypto Story: What’s Next?’ In: URL: <https://www.youtube.com/watch?v=culuNbMPPOk> (visited on 01/03/2022).
- Juvekar, Chiraag, Vinod Vaikuntanathan and Anantha P. Chandrakasan (2018). ‘Gazelle: A Low Latency Framework for Secure Neural Network Inference’. In: *CoRR* abs/1801.05507. arXiv: [1801.05507](https://arxiv.org/abs/1801.05507). URL: <http://arxiv.org/abs/1801.05507>.
- Laine, Kim (2020). *Result Ciphertext is Transparent*. GitHub. URL: <https://github.com/microsoft/SEAL/issues/224#issuecomment-702516479> (visited on 04/03/2022).
- LeCun, Yann and Corinna Cortes (1998). *The MNIST database of handwritten digits*. URL: <http://yann.lecun.com/exdb/mnist/>.
- Nüst, Daniel, Vanessa Sochat, Ben Marwick, Stephen J. Eglen, Tim Head, Tony Hirst and Benjamin D. Evans (2020). ‘Ten simple rules for writing Dockerfiles for reproducible data science’. In: *PLOS Computational Biology* 16.11, e1008316. DOI: [10.1371/journal.pcbi.1008316](https://doi.org/10.1371/journal.pcbi.1008316).
- Shannon, Claude E. (1949). ‘Communication Theory of Secrecy Systems’. In: *Bell System Technical Journal* 28.4, pp. 656–715. DOI: [10.1002/j.1538-7305.1949.tb00928.x](https://doi.org/10.1002/j.1538-7305.1949.tb00928.x).

List of Figures

- 2.1 Ah yes the caption 6
- 2.2 Comparison of the Relu activation function vs. its Taylor expansion 7
- 3.1 Image source: [Juvekar, Vaikuntanathan and Chandrakasan 2018](#) 11

List of Tables