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, Month 2020

Abstract

Abstract of your thesis (at most one page)

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer 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

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:

$$\mathcal{E}(m_1) \cdot \mathcal{E}(m_2) = (m_1)^r (m_2)^r \mod n \tag{2.1}$$
$$= (m_1 m_2)^r \mod n \tag{2.2}$$
$$= \mathcal{E}(m_1 \cdot m_2) \tag{2.3}$$

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

> **Definition 2.1.1: G**ven two rings $(R, +, \cdot)$ and $(S, \oplus, \otimes)$, we call a mapping $\varphi : R \to S$ a ring homomorphism, when it satisfies the following conditions:
>
> $$\forall a, b \in R : \varphi(a + b) = \varphi(a) \oplus \varphi(b) \wedge \varphi(a \cdot b) = \varphi(a) \otimes \varphi(b)$$
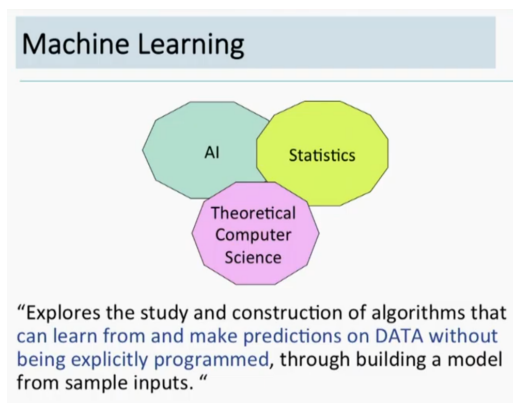
2.1.3 Learning with Errors (LWE)

2.1.4 Ring-LWE

Learning with Errors on Rings (RLWE)

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.

Machine Learning

"Explores the study and construction of algorithms that can learn from and make predictions on DATA without being explicitly programmed, through building a model from sample inputs."

2.2 Machine Learning

As Shafi Goldwasser puts it, 'Machine Learning is somewhere in the intersection of Artificial Intelligence, Statistics and Theoretical Computer Science' [Gol18].

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.
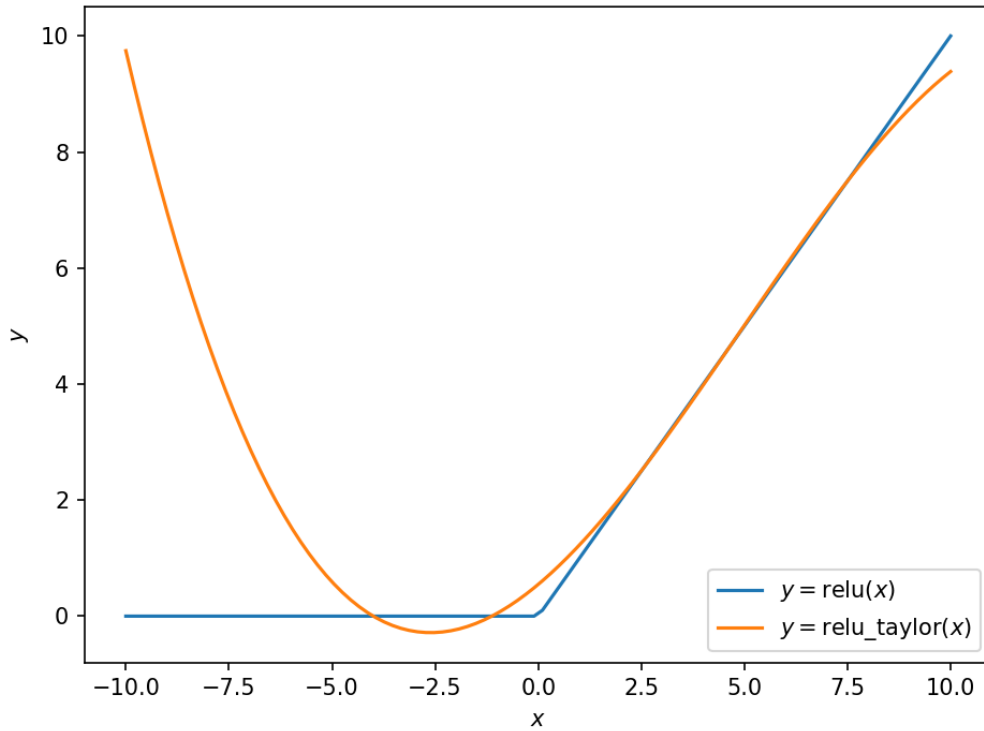
Figure 2.1: Comparison of the Relu activation function vs. its Taylor expansion

2.5 Notation and Acronyms

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

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

2.6 Citations

This is an example of how to specify and cite a book [DR02], a journal article [Sha49]. We can also add the authors' names to the citation: AES is a block cipher defined by Daemen and Rijmen [DR02].

Performance

Chapter 3

Conclusion

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer 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

Acronyms

Bibliography

[DR02]   Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES – The Advanced Encryption Standard.* Information Security and Cryptography. Springer, 2002. ISBN: 3-540-42580-2. DOI: 10.1007/978-3-662-04722-4.

[Gol18] Shafi Goldwasser. 'From Idea to Impact, the Crypto Story: What's Next?' In: (2018).

[Sha49] Claude E. Shannon. 'Communication Theory of Secrecy Systems'. In: *Bell System Technical Journal* 28.4 (1949), pp. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x.