IAIK

SCIENCE ▪ PASSION ▪ TECHNOLOGY

TU Graz

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)

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

This is the second paragraph. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Keywords: FHE, classification, neural network

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

Languages: C++, Python, JavaScript

Contents

1 Introduction

Goal:

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

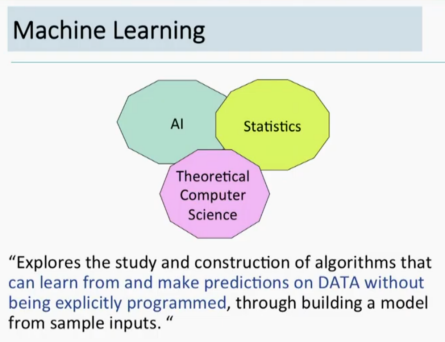
With unpadded RSA, some arithmetic can be performed on the ciphertext - looking at the encrypted ciphertext $\mathcal{E}(m_1) = (m_1)^r \mod n$ of the message m_1 and m_2 respectively, the following holds:

$$\begin{aligned} \mathcal{E}(m_1) \cdot \mathcal{E}(m_2) &= (m_1)^r (m_2)^r \mod n && (2.1)\\ &= (m_1 m_2)^r \mod n && (2.2)\\ &= \mathcal{E}(m_1 \cdot m_2) && (2.3) \end{aligned}$$

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

Definition 1 *Given 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.

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.

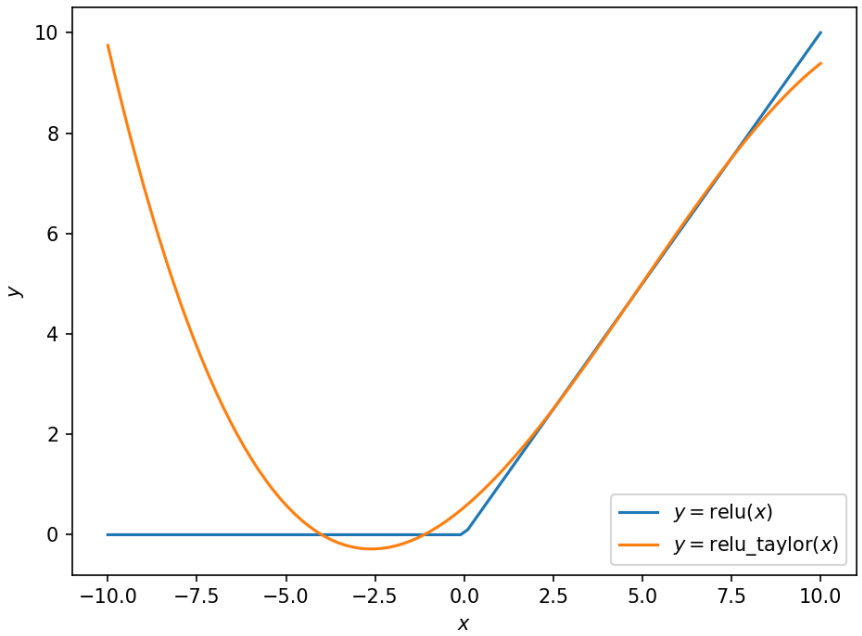


Figure 2.1: Comparison of the Relu activation function vs. its Taylor expansion

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], a conference article [**spKocherHFGGHHLM019**], and an informal report [**iacrSchneierFKR15**]. We can also add the authors' names to the citation: AES is a block cipher defined by Daemen and Rijmen [DR02].

Performance

3 Conclusion

And after the second paragraph follows the third paragraph. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

After this fourth paragraph, we start a new paragraph sequence. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Notation

$\oplus$	exclusive-or (Xor)	7

Acronyms

AES	Advanced Encryption Standard	7
FHE	Fully Homomorphic Encryption	5
HE	Homomorphic Encryption	5

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.