KU LEUVEN

FACULTY OF
ENGINEERING SCIENCE

# The best master's thesis ever

First Author
Second Author

Thesis submitted for the degree of
Master of Science in
Electrical Engineering, option
Electronics and Chip Design

*Supervisor*
Prof. dr. ir. Knows Better

*Assessors*
Ir. Kn. Owsmuch
K. Nowsrest

*Assistant-supervisors*
Ir. An Assistent
A. Friend

Academic year 2025 – 2026

Published by First Author and Second Author,
Department of Electrical Engineering, Kasteelpark Arenberg 10 bus 2440, B-3001 Leuven

# Preface

I would like to thank everybody who kept me busy the last year, especially my promoter and my assistants. I would also like to thank the jury for reading the text. My sincere gratitude also goes to my wive and the rest of my family.

*First Author*
*Second Author*

# Contents

# Abstract

The `abstract` environment contains a more extensive overview of the work. But it should be limited to one page.

# List of Figures and Tables

## List of Figures

## List of Tables

# List of Abbreviations and Symbols

## Abbreviations

| | |
|---|---|
| LoG | Laplacian-of-Gaussian |
| MSE | Mean Square error |
| PSNR | Peak Signal-to-Noise ratio |

## Symbols

| | |
|---|---|
| $c$ | Speed of light |
| $E$ | Energy |
| $m$ | Mass |
| $\pi$ | The number pi |

# Chapter 1

# Introduction

The first contains a general introduction to the work. The goals are defined and the modus operandi is explained.

## 1.1 Lorem Ipsum 4–5

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer 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 consectetuer.

## 1.2 Lorem Ipsum 6–7

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.

# Chapter 2

# Theoretical background

xxxx

## 2.1 Homomorphic encryption

So far, encryption technologies are shown to be effective to protect stored and in transit data. However, when data is used for computation, preserving privacy becomes more complex. To achieve this, several privacy-enhancing technologies (PETs) are available. One type of PET is homomorphic encryption (HE), which allows computation on encrypted data without decrypting. No party performing computations has access to the plaintext data, these data remains encrypted. Partially homomorphic encryption (PHE) is a type of HE that only supports homomorphic multiplication or addition, but not both. Full HE (FHE) and Somewhat HE (SHE) support both multiplications and additions, but with SHE only up to a limited computation depth. To enhance security, noise is added to the encrypted data when using HE, in the least significant bits as illustrated in figure 2.1. However, when performing computations the noise can grow beyond the noise padding bits, eventually corrupting the data in SHE. To mitigate this, bootstrapping can be performed in FHE to reduce the amount of noise, thus allowing more computations to be done whilst maintaining data integrity.

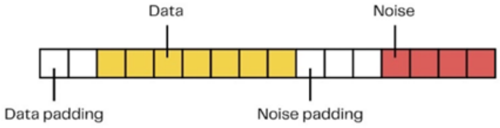

FIGURE 2.1: Ciphertext HE [5]

FHE offers strong advantages when compared to other PETs. For instance, less communication is needed during computation when compared to MPC (multi-party computation) and it has a better track record in terms of security vulnerability when compared to TEE (trusted execution environment). [6]

On the other hand, there are some disadvantages too. FHE requires requires specialized expertise to implement. But, most importantly, FHE is computationally intensive (thus slow) for large and unstructured data. According to Ulf Mattsson, general FHE processing is 1.000 to 1.000.000 times slower than equivalent plaintext operations. [11]

Whilst performing a large number of (complex) operations, noise added to the HE cyphertext will grow and overwrite data. To avoid this, two methods are used: using big integers and bootstrapping. By using big integers, enough space is provided for the noise to grow for the full computation - the so called leveled schemes. [1] To have more computation depth possible, bootstrapping operations are performed to reduce the amount of noise in between chains of computations. One should note bootstrapping is computationally and memory-intensive.

FHE schemes can be divided into multiple generations, depending on the type of bootstrapping techniques. [3] First generation schemes include schemes like the Gen09 bootstrapping technique, described in 2009, which is illustrated in figure 2.2. FHE-encrypted data are FHE-encrypted a second time, with a lower level of noise compared to the initial encryption. Then, a bootstrapping key is sent to the computing node, which is the secret key of the initial encryption, encrypted with the public key of the second encryption. Decryption with this bootstrapping key removes the first encryption layer, and one ends up with data solely encrypted via the second FHE-scheme, with a lower level of noise. This type of scheme is no longer used in practical implementations.

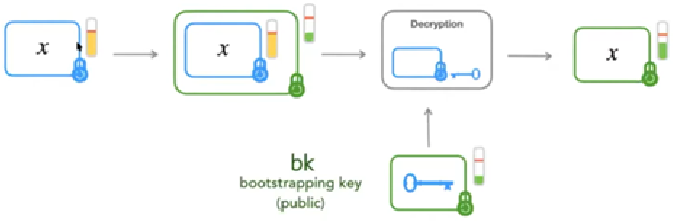

Figure 2.2: Gen09 bootstrapping [5]

Second generation schemes are defined by having a slow and complex bootstrapping. However, bootstrapping cost is compensated by the use of SIMD (Single Instruction Multiple Data) operations, which will distribute this cost over many slot, so many parallel computations. Examples are BGV, BFV and CKKS. Third generation schemes are characterized by a very simple and fast bootstrapping procedure. These exhibit lower circuit complexity, faster execution times, and less noise growth when compared to second generation. On the contrary, they will not offer SIMD slots for parallel processing. Examples include torus FHE (TFHE).

Next to these generations, some FHE leveled homomorphic encryption schemes where no bootstrapping technique is known for the moment. The CLPX scheme fro Chen et al. [1] is an example, where the parameters of the scheme are set as such level to allow deep circuit evaluation before noise corrupts the result.

[1] BFV and CKKS are often implemented without bootstrapping, as a leveled scheme, but are bootstrappable.

### 2.1.1 General-BFV

The BFV (Brakerski–Fan–Vercauteren) scheme is

#### Cyclotomic rings

BFV is built on the RLWE problem (ring learning with errors), which is a hardness problem used in cryptography. We define the m-th cyclotomic polynomial as follows:

$$\Phi_m(x) = \prod_{j \in \mathbb{Z}_m^\times} \left(x - \omega_m^j\right)$$

- $w_m$ is the primitive $m$-th root of unity, $\in \mathbb{C}$ where $m \geq 1$
- $\mathbb{Z}_m^\times$ is the unity group of integer modulo $m$.

The degree of the cyclotomic polynomial is equal to $\varphi(m)$, the result of the Euler's totient function of m. Although the cyclotomic polynomial have complex roots, it has been proven that the coefficients are integer numbers and the polynomials are monic (leading coefficient is 1) and irreducible. The RLWE problem is then defined over the ring $\mathcal{R} = Z[x]/(\phi_m(x)$. This ring is a subring of the cyclotomic number field $\mathbb{Q}[x]/(\Phi_m(x))$.

#### R-LWE

**LWE:** The ciphertext is constituted of two parts: uniform random numbers $a_i$ and $b$, where $b$ is the sum of the multiplication of the uniform random numbers $a_i$ with the secret key $s_i$, some Gaussian distributed noise $e$ and the message $m$, normalized by a delta coefficient. The corresponding ciphertext can be represented on a ring, all the possible values of m are put on a ring, at a spacing delta from each other. To decrypt, the decryption formula (2.2) is used, which is equivalent to rounding the value on the ring (which corresponds to delta times the message plus the error) to the closest possible value for m. If the error becomes too large, the value will round to the wrong message value, so returning a faulty message.

$$\text{Encryption:} \quad ct = (a_0, \ldots, a_{n-1}, b) \quad where \quad b = \sum_{i=0}^{n-1} a_i s_i + e + \Delta m \tag{2.1}$$

$$\text{Decryption:} \quad m \approx \frac{b - \mathbf{a} \cdot \mathbf{s}}{\Delta} \tag{2.2}$$

$a_i \in \mathbb{Z}_q$ are chosen uniformly at random
$s_i \in \mathbb{Z}_q$ are the secret key coefficients
$e \in \mathbb{Z}_q$ is a small error term (typically Gaussian)
$m$ is the message encoded in the ring
$\Delta$ is the message scaling factor

$b \in \mathbb{Z}_q$ is the second component of the ciphertext

This scheme already allows to do some operations on the ciphertext: we can add two ciphertexts and perform multiplications of the ciphertext with non-encrypted integers.[2]

**RLWE:** Ring LWE is similar to LWE but it will, when constructing the ciphertext, use polynomial modulo's instead (for the message, secret key, uniform random numbers and error). When encrypting, we will normalize the message and add a Gaussian error, like in LWE. For every coefficient of the polynomial, the value of delta m plus the error will again be represented on a ring. Rounding will give the polynomial coefficients of the message m. The RLWE scheme allows to perform additions between ciphertexts and multiplication with non-encrypted constant polynomial functions.

The RLWE problem is based on the RLWE distribution for integers $q \geq 2$ and a secret s sampled from $\chi_{key}$. The decision RLWE problem is, given many plaintext-ciphertext samples, to decide whether the samples come from a uniform random distribution or from the RLWE distribution. When solving the search RLWE problem, many plaintext-ciphertexts are given from the RLWE distribution, and one needs to find the secret s. Both variants are supposed to be hard.

### BFV, CLPX and SIMD

In BFV by Kim et al.[7], a subring $\mathcal{R}_t$ of $\mathcal{R}$ is ceated by taking modulo t of rhe ring $\mathcal{R}$. In the case of BFV, we fix this $t$ to the prime integer $p$. The ciphertext also has a modulus q and the message is scaled by a factor $\delta = q/t$. The plaintext space corresponds to $R_t = \mathbb{Z}[x]/(\Phi_m(x), p)$. Encryption is then done via following formula:

$$\text{Ciphertext:} \quad \mathbf{ct} = \left(\left[\lfloor \Delta \cdot m \rceil + \mathbf{a} \cdot \mathbf{s} + e\right]_q, -\mathbf{a}\right) \tag{2.3}$$

$$\text{Decryption:} \quad m = \left\lfloor \frac{c_0 + c_1 \cdot \mathbf{s}}{\Delta} \right\rceil \tag{2.4}$$

And decryption: The scheme can be implemented as a leveled scheme (SHE) or can be bootstrapped to a fully homomorphic encryption scheme.In BFV, one can perform addition, multiplication and automorphism over the plaintext space.

### Slots

Smart and Vercauteren [14] noticed that it was possible to encode multiple elements in one plaintext, using the Chinese Remainder Theorem. This splitting in splots can allow SIMD operation - performing a single operation on multiple data.

BFV can support packing in slots and thus SIMD operations. However, doing this puts a restriction on the use of BFV. If $p$ is the modulus of the plaintext $(\phi_m(b))$, the upper bound of the output noise will grow proportional to to the

[2] An operation on ciphertexts will, in FHE, correspond to an operation on plaintexts.

product of this factor and the sum of the upper bounds on the input noise. When one wants to have a high precision arithmetic, one chooses a high p, which will result in more output noise. This makes SIMD-schemes impractical when performing precise arithmetic calculations, often needed in HE-applications. For instance, privacy-preserving machine learning uses moduli up to 80 bits.[4] Also, a higher value of $p$ enables a higher packing density. The packing density, which is equal to the number of slots divided by the ring dimension, is equal to $1/d$. $D$ is the multiplicative order of $p$ modulo the cyclotomix index $m$. To achieve full packing, $p$ needs to be larger then $m$. When using power-of-two cyclotomics, the number of slots will be upper bounded by $(p{+}1)/2$. To conclude, while a large value of $p$ allows for greater packing density and more precise arithmetic operations, it simultaneously exacerbates noise growth.

In CLPX, the idea is to use a plaintext ring modulo $t$, with $t = x - b$ instead of an integer $p$, as in BFV. The plaintext space is now defined as

$$\mathcal{R}_t = \mathbb{Z}[x]/(\Phi_m(x), x - b) = \mathbb{Z}[x]/(x - b, p) \cong \mathbb{Z}_p \tag{2.5}$$

In this CLPX-scheme, $m$ is a $k$-th power of 2. When encrypting first a hat encoding is performed on the message m, by taking the modulus quotient ring of R modulo t. We get $\hat{m}$ which only has small coefficients. Encryption is done as follows:

$$\mathbf{c} = \left(\left[\Delta \cdot \hat{m} + \mathbf{a} \cdot \mathbf{s} + e\right]_q, -\mathbf{a}\right) \tag{2.6}$$

Decryption is performed using the secret key $\mathbf{s}$:

$$\hat{m} = \left\lfloor \frac{t}{q} \cdot \left(c_0 + c_1 \cdot \mathbf{s}\right) \right\rceil \tag{2.7}$$

In CLPX, addition and multiplication can be performed homomorphically.[1].

CLPX can encrypt a single huge integer modulo $\phi_m(b)$ and has much lower noise growth when compared to BFV - the growth is sublinear in $b$ (instead of $\phi_m(b)$). This makes CLPX suitable for high-precision arithmetic HE operations. However, in CLPX Only a single element is encrypted, so no SIMD operations can be performed. Also, since the size of $p$ is exponential in $m$, there are no known bootstrapping techniques for CLPX.

### 2.1.2 GBFV

CLPX has much lower noise growth when compared to BFV, but does not support SIMD operations and is not known to be efficiently bootstrappable for cryptographically secure parameters. Geelen and Vercauteren propose the GBFV scheme which combines the SIMD and bootstrapping capabilities of BFV with the lower noise growth of CLPX, by tuning the parameters $m$ and $t(x)$. Combing both properties would either yield a scheme capable of evaluating deeper circuits or would yield a scheme capable of working with smaller ring dimensions.

GBFV operates over the cyclotomic ring $\mathcal{R} = \mathbb{Z}[x]/\phi_m(x)$. The plaintext space is defined modulo an arbitrary non-zero principal ideal generated by a polynomial

$t = t(x)$. This ring is $R_t = R/tR$. A plaintext $m \in \mathcal{R}_{\sqcup}$ is encrypted into a ciphertext $ct \in \mathcal{R}^{\in}_{\amalg}$ with RLWE:

$$ct = \Big( \big[ \lfloor \Delta \cdot m \rceil + a \cdot s + e \big]_q ,\ -a \Big) \text{[3]} \tag{2.8}$$

The ciphertext space will be a ring $\mathcal{R}^2_q$ with $q \geq 2$. The scaling factor $\Delta$ is defined by $q/t$, with $q$ the ciphertext modulus. This scaling factor is not rounded to $\mathcal{R}$, resulting in a conceptually simples scheme definition when compared to BFV and CLPX.

For correct decryption, the canonical infinity norm of the plaintext modulus must be much smaller then the ciphertext modulus. This ensures that the decryption correctly recovers plaintexts without modular wrap-around or rounding errors, all contributions from $t(x)$ (i.e. $t(x) * m(x)$) and the noise much be much smaller than q.

### 2.1.3 Scheme functions

The GBFV scheme has several functions which it can perform:

- Secret key generation: Samples a secret key $s$ from a key distributon $\chi_{key}$, $s \in \mathcal{R}$, returns s.

- Relinearization key: after multiplication of ciphertexts, one gets a higher order polynomial in $s$, which can not be decrypted since the scheme only knows $s$ and not $s$ to a higher power. The relinearization key approximates the ciphertext back to a linear equation in s. Returns the evaluation key.

- Decryption: A ciphertext is decrypted using $m = \left\lfloor \frac{c_0 + c_1 \cdot s}{\Delta} \right\rceil$. Returns $m$.

GBFV supports standard homomorphic operations on ciphertexts, using following functions:

- Ciphertext-ciphertext addition: ciphertext addition is done component-wise modulo $q$ and returns $ct_{add}$.

- Plaintext-ciphertext addition: the plaintext is encrypted as follows:

  $$ct' = \Big( \big[ \lfloor \Delta \cdot m \rceil \big]_q ,\ 0 \Big)$$

  After this stage, add the original ciphertext with $ct'$ (ciphertext-ciphertext addition).

- Key switching: reduces the result of the ciphertext-ciphertext multiplication back to two components.

[3] $\lfloor x \rceil$ is rounding to the nearest integer

- Ciphertext-ciphertext multiplication: two ciphertexts $ct(c_0, c_1)$ and $ct' = (c'_0, c'_1)$ are multiplied as follows:

$$\mathbf{c}'' = \Big( [\lfloor \frac{c_0 \cdot c'_0}{\Delta} \rceil]_q, \; [\lfloor \frac{c_0 \cdot c'_1 + c_1 \cdot c'_0}{\Delta} \rceil]_q \Big), \tag{2.9}$$

$$c''_2 = \Big[ \lfloor \frac{c_1 \cdot c'_1}{\Delta} \rceil \Big]_q \tag{2.10}$$

  Since the $c''_2$ contains a second-order term in s, a relinearization is performed using the relinearization key, creating $ct'''$. This ciphertext is then added to $ct''$.

- Ciphertext-plaintext multiplication: takes the ciphertext and multiplies both parts with the flattened message $m$ [4]

- Automorphism. Applying an automorphism to the ciphertext polynomials, this permutes slots in packed plaintexts after decryption. Then, the plaintext moduli are corrected if they changed under the automorphism. A key switching is performed to bring back the secret key to s. Finally, the adjusted ciphertexts are combined to form the final output.

### 2.1.4 SIMD

## 2.2 Private information retrieval

When retrieving information from a remote server, the database holder will know which elements are queried. To protect the user, one wants to hide which elements are queried from the server. Private information retrieval or PIR is often considered to achieve this goal.

Private information retrieval (PIR) is the process where a user retrieves information from a database without revealing to the database what he is retrieving. The goal is to ensure the server does not learn anything about the index from the user query. This will enhance the privacy of the user, since no information will be leaked to the (remote) server(s), potentially causing serious privacy issues. PIR finds application in multiple scenarios where sensitive data are used. For example, a doctor querying a database with patient's medical data will get back the requested medical information, without the server learning which patient or which patient record was requested. PIR also finds applications in technology. Apple uses PIR to provide caller ID information of an incoming phone call, without them learning who is calling who [10].

[4] Flattening involves reducing the coefficients from, ensuring the coefficients are reduced modulo $t$ but expressed in $\mathcal{R}$. Following formula is used:

$$\text{Flatten} : \mathcal{R}_t \to \mathcal{R} : \quad m \mapsto t \cdot [\frac{m}{t}]_1$$

PIR protocols can be categorized in two groups: single-server PIR and multi-server PIR. The single-server PIR is the most straightforward setting: one server holds the full dataset, and the client queries the server to get the data of interest. In multi-server PIR, there are multiple servers holding a copy of the full dataset, and the client queries multiple servers to obtain the data of interest. The core idea when using multi-server PIR is that, although the dataset is replicated on multiple servers, the query is split into parts. In this way, none of the servers learn which bit is requested but the requested bit can be recovered from the results of the different servers.

$$\textbf{Database: } D = [\, b_1, \, b_2, \, b_3, \, b_4 \,]$$

The client wants to retrieve $b_3$ privately.

—

**Step 1: Query generation**

The client samples a random binary vector:

$$q_1 = [\, q_{11}, \, q_{12}, \, q_{13}, \, q_{14} \,]$$

and constructs

$$q_2 = q_1 \oplus e_3$$

where

$$e_3 = [\, 0, \, 0, \, 1, \, 0 \,]$$

is the unit vector with a 1 in the 3rd position.

The client sends:

$$q_1 \text{ to Server 1}, \quad q_2 \text{ to Server 2}.$$

—

**Step 2: Servers compute answers**

Each server computes the XOR of the database entries where its query has 1s:

$$a_1 = q_1 \cdot D = \bigoplus_{j=1}^{4} (q_{1j} \cdot b_j)$$

$$a_2 = q_2 \cdot D = \bigoplus_{j=1}^{4} (q_{2j} \cdot b_j)$$

—

**Step 3: Client combines responses**

$$a_1 \oplus a_2 = \left( \bigoplus_{j=1}^{4} (q_{1j} \cdot b_j) \right) \oplus \left( \bigoplus_{j=1}^{4} (q_{2j} \cdot b_j) \right) = b_3$$

—

Client learns $b_3$, and neither server learns which $b_i$ was requested.

Security holds as long as the servers do not collude. This assumption is difficult to achieve, because the database has to be on multiple servers, but one party can not have control over these servers. Therefore, single-server PIR schemes are often preferred since they rely on cryptographic hardness assumptions, but at the cost of incurring a huge performance overhead. In this thesis, we will further focus on single-server PIR.

A scheme is information-theoretic secure when the queries asked by the user give no information whatsoever about the requested bit. For a single-server PIR scheme, the trivial information-theoretic secure scheme is sending the whole database to the client, he can then query the database and the server will have no information about the selected bit. This gives a communication of O(n). Single-server PIR schemes with smaller communication cost are computationally secure, not information-theoretic secure. [2] [9] [13] Kushilevitz and Ostrovsky made use of the number-theoretic assumption to deduce a single-server computationally secure PIR with subpolynomial communication. The scheme has a communication complexity of O(n to the epsilonth) for any epsilon > 0. This scheme however requires n big integer multiplications. Cachin et al. proposed a two-round computationally secure PIR using the phi-hiding assumption where communication complexity is polylogarithmic in n. This scheme requires n modular exponentiations, with large moduli, which makes multiplication slower then in Kuhilevitz's scheme. Chang subsequently proposed a scheme with logarithmic communication complexity, using Paillier's cryptosystem. As Sion and Carbunar pointed out, these single-server PIR protocols are mostly orders of magnitude slower than the trivial transfer of the entire database to the client.

FHE-based PIR allows computation over encrypted data and offers optimal communication and computation complexity.

## 2.3 Feanor-math and feanor

Feanor-math and feanor are bothe rust libraries made by Simon Pohmann a PhD student at Royal Holloway, University of London. Hise filed of studie is criptographie and computational mathematics. [12] Feanor-mat is a library for number theory, and feanor is a library that provides implementions of building blocks for HE, build on feanor-math.

### 2.3.1 Feanor-math

Like mentiond before feanor-math is a library for number theory. The librari is complietly rithen in rust. The library starts from a main trait[5] `Ring`, and then

[5] Trait definitions are a way to group method signatures together to define a set of behaviors necessary to accomplish some purpose.[8]

creathes a thread yiarchie for additional properties.

## Chapter 3

# The Next Chapter

Vivamus adipiscing. Curabitur imperdiet tempus turpis. Vivamus sapien dolor, congue venenatis, euismod eget, porta rhoncus, magna. Proin condimentum pretium enim. Fusce fringilla, libero et venenatis facilisis, eros enim cursus arcu, vitae facilisis odio augue vitae orci. Aliquam varius nibh ut odio. Sed condimentum condimentum nunc. Pellentesque eget massa. Pellentesque quis mauris. Donec ut ligula ac pede pulvinar lobortis. Pellentesque euismod. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent elit. Ut laoreet ornare est. Phasellus gravida vulputate nulla. Donec sit amet arcu ut sem tempor malesuada. Praesent hendrerit augue in urna. Proin enim ante, ornare vel, consequat ut, blandit in, justo. Donec felis elit, dignissim sed, sagittis ut, ullamcorper a, nulla. Aenean pharetra vulputate odio.

## 3.1 The First Topic of this Chapter

Quisque enim. Proin velit neque, tristique eu, eleifend eget, vestibulum nec, lacus. Vivamus odio. Duis odio urna, vehicula in, elementum aliquam, aliquet laoreet, tellus. Sed velit. Sed vel mi ac elit aliquet interdum. Etiam sapien neque, convallis et, aliquet vel, auctor non, arcu. Aliquam suscipit aliquam lectus. Proin tincidunt magna sed wisi. Integer blandit lacus ut lorem. Sed luctus justo sed enim.

### 3.1.1 An item

A master's thesis is never an isolated work. This means that your text must contain references. On-line documents as well as can be referenced.

Usually a text also contains inline formulas ($\sin^2\eta + \cos^2\eta = 1$) or formulas as separate equations.

$$\sigma(t) = \frac{1}{\sqrt{2\pi}} \int_0^t e^{-x^2/2} dx \tag{3.1}$$

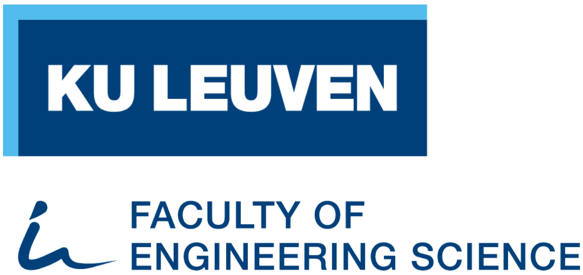

Figure 3.1: The logo of the Faculty of Engineering Science.

| | | |
|---|---|---|
| gnats | gram | $13.65 |
| | each | .01 |
| gnu | stuffed | 92.50 |
| emu | | 33.33 |
| armadillo | frozen | 8.99 |

Table 3.1: A table with the wrong layout.

| Item | | |
|---|---|---|
| Animal | Description | Price ($) |
| Gnat | per gram | 13.65 |
| | each | 0.01 |
| Gnu | stuffed | 92.50 |
| Emu | stuffed | 33.33 |
| Armadillo | frozen | 8.99 |

Table 3.2: A table with the correct layout.

## 3.2 Figures

Figures are used to add illustrations to the text. The Figure 3.1 shows the KU Leuven logo as an illustration.

## 3.3 Tables

Tables are used to present data neatly arranged. A table is normally not a spreadsheet! Compare Table 3.1 en Table 3.2: which table do you prefer?

## 3.4 Lorem Ipsum

This section is added to check headers and footers. So this chapter must at least contain three pages. To make sure that we get the required amount, the lipsum package isn't used but the text is put directly in the text.

### 3.4.1 Lorem ipsum dolor sit amet, consectetur adipiscing elit

Sed nec tortor id felis tristique sodales. Nulla nec massa eu dui fermentum tincidunt. Integer ullamcorper ante eget eros posuere faucibus. Nam id ligula ut augue pulvinar vulputate id at purus. Aenean condimentum tortor eu mi placerat eget eleifend massa mollis. Nam est mi, sagittis quis euismod eget, sagittis in nibh. Proin elit turpis, aliquam et imperdiet sed, volutpat eu turpis.

Pellentesque vel enim tellus, vitae egestas turpis. Praesent malesuada elit non nisi sollicitudin non blandit lacus tincidunt. Morbi blandit urna at lectus ornare laoreet. Suspendisse turpis diam, lobortis dictum luctus quis, commodo at lorem. Integer lacinia convallis ultricies. Sed quis augue neque, eu malesuada arcu. Nullam vehicula, purus vitae sagittis pulvinar, erat eros semper massa, eu egestas nibh erat quis magna. Cras pellentesque, nisl eu dapibus volutpat, urna augue ornare quam, quis egestas lectus nulla a lectus.

Vivamus dictum libero in massa cursus sed vulputate eros imperdiet. Donec lacinia, libero ac lobortis egestas, nibh dui ornare arcu, luctus porttitor velit massa sit amet quam. Maecenas scelerisque laoreet diam, vitae congue quam adipiscing vitae. Aliquam cursus nisl a leo convallis eleifend fermentum massa porta. Nunc libero quam, dapibus dapibus molestie sit amet, faucibus vel nunc.

### 3.4.2 Praesent auctor venenatis posuere

Sed tellus augue, molestie in pulvinar lacinia, dapibus non ipsum. Fusce vitae mi vitae enim ullamcorper hendrerit eu malesuada est. Proin iaculis ante sed nibh tincidunt vel interdum libero posuere. Vivamus accumsan metus quis felis congue suscipit dapibus enim mattis. Fusce mattis tortor eget ipsum interdum sagittis auctor id metus.

Integer diam lacus, pharetra sit amet tempor et, tristique non lorem. Aenean auctor, nisi eu interdum fermentum, lectus massa adipiscing elit, sed facilisis orci odio a lectus. Proin mi nibh, tempus quis porta a, viverra quis enim. In sollicitudin egestas libero, quis viverra velit molestie eget. Nulla rhoncus, dolor a mollis vestibulum, lacus elit semper nisi, nec sollicitudin sem urna eu magna. Nunc sed est urna, euismod congue mi.

### 3.4.3 Cras vulputate ultricies venenatis

Vivamus eros urna, sodales accumsan semper vel, lobortis sit amet mauris. Etiam condimentum eleifend lorem, ullamcorper ornare lectus aliquet vitae. Praesent massa enim, interdum sit amet semper et, venenatis ut elit. Quisque faucibus, quam ac lacinia imperdiet, nulla neque elementum purus, tempus rutrum justo massa porta sapien. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Sed ultrices interdum mi, et rhoncus sapien rutrum sed.

Duis elit orci, molestie quis sollicitudin sed, convallis non ante. Maecenas tincidunt condimentum justo, et ultricies leo tristique vitae. Vestibulum quis quam non lectus dapibus eleifend a vitae nibh. Nam nibh justo, pharetra quis iaculis consequat, elementum quis justo. Etiam mollis lacinia lacus, nec sollicitudin urna lobortis ac. Nulla facilisi.

Proin placerat risus eleifend erat ultricies placerat. Etiam rutrum magna nec turpis euismod consectetur. Phasellus tortor odio, lacinia imperdiet condimentum sed, faucibus commodo erat. Phasellus sed felis id ante placerat ultrices. Aenean tempor justo in tortor volutpat eu auctor dolor mollis. Aenean sit amet risus urna. Morbi viverra vehicula cursus.

### 3.4.4 Donec nibh ante, consectetur et posuere id, tempus nec arcu

Curabitur a tellus aliquet ipsum pellentesque scelerisque. Etiam congue, risus et volutpat rutrum, est purus dapibus leo, non cursus metus felis eget ligula. Vivamus facilisis tristique turpis, ut pretium lectus luctus eleifend. Fusce magna sapien, ullamcorper vitae fringilla id, euismod quis ante.

Phasellus volutpat, nunc et pharetra semper, sem justo adipiscing mauris, id blandit magna quam et orci. Vestibulum a erat purus, ut molestie ante. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Proin turpis diam, consequat ut ullamcorper ut, consequat eu orci. Sed metus risus, fringilla nec interdum vel, interdum eu nunc. Suspendisse vel sapien orci.

### 3.4.5 Morbi et mauris tempus purus ornare vehicula

Mauris sit amet diam quam, eget luctus purus. Sed faucibus, risus semper eleifend iaculis, mi turpis bibendum nisl, quis cursus nibh nisl sit amet ipsum. Vestibulum tempor urna vitae mi auctor malesuada eget non ligula. Nullam convallis, diam vel ultrices auctor, eros eros egestas elit, sed accumsan arcu tortor eget leo. Vestibulum orci purus, porttitor in pharetra eget, tincidunt eget nisl. Nullam sit amet nulla dui, facilisis vestibulum dui.

Donec faucibus facilisis mauris ac cursus. Duis rhoncus quam sed nisi laoreet eu scelerisque massa tincidunt. Vivamus sit amet libero nec arcu imperdiet tempor quis non libero. Sed consequat dignissim justo. Phasellus ullamcorper, velit quis posuere vulputate, felis erat tincidunt mauris, at vestibulum justo lectus et turpis. Maecenas lacinia convallis euismod. Quisque egestas fermentum sapien eu dictum. Sed nec lacus in purus dictum consequat quis vel nisl. Fusce non urna sem. Curabitur eu diam vitae elit accumsan blandit. Nullam fermentum nunc et leo dictum laoreet. Donec semper varius velit vel fringilla. Vivamus eu orci nunc.

## 3.5 Conclusion

The final section of the chapter gives an overview of the important results of this chapter. This implies that the introductory chapter and the concluding chapter don’t need a conclusion.

Nunc sed pede. Praesent vitae lectus. Praesent neque justo, vehicula eget, interdum id, facilisis et, nibh. Phasellus at purus et libero lacinia dictum. Fusce aliquet.

Nulla eu ante placerat leo semper dictum. Mauris metus. Curabitur lobortis. Curabitur sollicitudin hendrerit nunc. Donec ultrices lacus id ipsum.

Chapter 4

# The Final Chapter

Morbi malesuada hendrerit dui. Nunc mauris leo, dapibus sit amet, vestibulum et, commodo id, est. Pellentesque purus. Pellentesque tristique, nunc ac pulvinar adipiscing, justo eros consequat lectus, sit amet posuere lectus neque vel augue. Cras consectetuer libero ac eros. Ut eget massa. Fusce sit amet enim eleifend sem dictum auctor. In eget risus luctus wisi convallis pulvinar. Vivamus sapien risus, tempor in, viverra in, aliquet pellentesque, eros. Aliquam euismod libero a sem.

## 4.1 The First Topic of this Chapter

### 4.1.1 Item 1

**Sub-item 1**

Nunc velit augue, scelerisque dignissim, lobortis et, aliquam in, risus. In eu eros. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Curabitur vulputate elit viverra augue. Mauris fringilla, tortor sit amet malesuada mollis, sapien mi dapibus odio, ac imperdiet ligula enim eget nisl. Quisque vitae pede a pede aliquet suscipit. Phasellus tellus pede, viverra vestibulum, gravida id, laoreet in, justo. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Integer commodo luctus lectus. Mauris justo. Duis varius eros. Sed quam. Cras lacus eros, rutrum eget, varius quis, convallis iaculis, velit. Mauris imperdiet, metus at tristique venenatis, purus neque pellentesque mauris, a ultrices elit lacus nec tortor. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent malesuada. Nam lacus lectus, auctor sit amet, malesuada vel, elementum eget, metus. Duis neque pede, facilisis eget, egestas elementum, nonummy id, neque.

**Sub-item 2**

Proin non sem. Donec nec erat. Proin libero. Aliquam viverra arcu. Donec vitae purus. Donec felis mi, semper id, scelerisque porta, sollicitudin sed, turpis. Nulla in urna. Integer varius wisi non elit. Etiam nec sem. Mauris consequat, risus nec congue condimentum, ligula ligula suscipit urna, vitae porta odio erat quis sapien. Proin luctus leo id erat. Etiam massa metus, accumsan pellentesque, sagittis sit amet, venenatis nec, mauris. Praesent urna eros, ornare nec, vulputate eget, cursus sed, justo. Phasellus nec lorem. Nullam ligula ligula, mollis sit amet, faucibus vel, eleifend ac, dui. Aliquam erat volutpat.

### 4.1.2 Item 2

Fusce vehicula, tortor et gravida porttitor, metus nibh congue lorem, ut tempus purus mauris a pede. Integer tincidunt orci sit amet turpis. Aenean a metus. Aliquam vestibulum lobortis felis. Donec gravida. Sed sed urna. Mauris et orci. Integer ultrices feugiat ligula. Sed dignissim nibh a massa. Donec orci dui, tempor sed, tincidunt nonummy, viverra sit amet, turpis. Quisque lobortis. Proin venenatis tortor nec wisi. Vestibulum placerat. In hac habitasse platea dictumst. Aliquam porta mi quis risus. Donec sagittis luctus diam. Nam ipsum elit, imperdiet vitae, faucibus nec, fringilla eget, leo. Etiam quis dolor in sapien porttitor imperdiet.

## 4.2 The Second Topic

Cras pretium. Nulla malesuada ipsum ut libero. Suspendisse gravida hendrerit tellus. Maecenas quis lacus. Morbi fringilla. Vestibulum odio turpis, tempor vitae, scelerisque a, dictum non, massa. Praesent erat felis, porta sit amet, condimentum sit amet, placerat et, turpis. Praesent placerat lacus a enim. Vestibulum non eros. Ut congue. Donec tristique varius tortor. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Nam dictum dictum urna.

Phasellus vestibulum orci vel mauris. Fusce quam leo, adipiscing ac, pulvinar eget, molestie sit amet, erat. Sed diam. Suspendisse eros leo, tempus eget, dapibus sit amet, tempus eu, arcu. Vestibulum wisi metus, dapibus vel, luctus sit amet, condimentum quis, leo. Suspendisse molestie. Duis in ante. Ut sodales sem sit amet mauris. Suspendisse ornare pretium orci. Fusce tristique enim eget mi. Vestibulum eros elit, gravida ac, pharetra sed, lobortis in, massa. Proin at dolor. Duis accumsan accumsan pede. Nullam blandit elit in magna lacinia hendrerit. Ut nonummy luctus eros. Fusce eget tortor.

Ut sit amet magna. Cras a ligula eu urna dignissim viverra. Nullam tempor leo porta ipsum. Praesent purus. Nullam consequat. Mauris dictum sagittis dui. Vestibulum sollicitudin consectetuer wisi. In sit amet diam. Nullam malesuada pharetra risus. Proin lacus arcu, eleifend sed, vehicula at, congue sit amet, sem. Sed sagittis pede a nisl. Sed tincidunt odio a pede. Sed dui. Nam eu enim. Aliquam sagittis lacus eget libero. Pellentesque diam sem, sagittis molestie, tristique et, fermentum ornare, nibh. Nulla et tellus non felis imperdiet mattis. Aliquam erat volutpat.

## 4.3 Conclusion

Vestibulum sodales ipsum id augue. Integer ipsum pede, convallis sit amet, tristique vitae, tempor ut, nunc. Nam non ligula non lorem convallis hendrerit. Maecenas hendrerit. Sed magna odio, aliquam imperdiet, porta ac, aliquet eget, mi. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Vestibulum nisl sem, dignissim vel, euismod quis, egestas ut, orci. Nunc vitae risus vel metus euismod laoreet. Cras sit amet neque a turpis lobortis auctor. Sed aliquam sem ac elit. Cras velit lectus, facilisis id, dictum sed, porta rutrum, nisl. Nam hendrerit ipsum sed augue. Nullam scelerisque hendrerit wisi. Vivamus egestas arcu sed purus. Ut ornare lectus sed eros. Suspendisse potenti. Mauris sollicitudin pede vel velit. In hac habitasse platea dictumst.

Suspendisse erat mauris, nonummy eget, pretium eget, consequat vel, justo. Pellentesque consectetuer erat sed lacus. Nullam egestas nulla ac dui. Donec cursus rhoncus ipsum. Nunc et sem eu magna egestas malesuada. Vivamus dictum massa at dolor. Morbi est nulla, faucibus ac, posuere in, interdum ut, sapien. Proin consectetuer pretium urna. Donec sit amet nibh nec purus dignissim mattis. Phasellus vehicula elit at lacus. Nulla facilisi. Cras ut arcu. Sed consectetuer. Integer tristique elit quis felis consectetuer eleifend. Cras et lectus.

Ut congue malesuada justo. Curabitur congue, felis at hendrerit faucibus, mauris lacus porttitor pede, nec aliquam turpis diam feugiat arcu. Nullam rhoncus ipsum at risus. Vestibulum a dolor sed dolor fermentum vulputate. Sed nec ipsum dapibus urna bibendum lobortis. Vestibulum elit. Nam ligula arcu, volutpat eget, lacinia eu, lobortis ac, urna. Nam mollis ultrices nulla. Cras vulputate. Suspendisse at risus at metus pulvinar malesuada. Nullam lacus. Aliquam tempus magna. Aliquam ut purus. Proin tellus.

# Appendices

# Appendix A

# The First Appendix

Appendices hold useful data which is not essential to understand the work done in the master's thesis. An example is a (program) source. An appendix can also have sections as well as figures and references.

## A.1 More Lorem

Quisque facilisis auctor sapien. Pellentesque gravida hendrerit lectus. Mauris rutrum sodales sapien. Fusce hendrerit sem vel lorem. Integer pellentesque massa vel augue. Integer elit tortor, feugiat quis, sagittis et, ornare non, lacus. Vestibulum posuere pellentesque eros. Quisque venenatis ipsum dictum nulla. Aliquam quis quam non metus eleifend interdum. Nam eget sapien ac mauris malesuada adipiscing. Etiam eleifend neque sed quam. Nulla facilisi. Proin a ligula. Sed id dui eu nibh egestas tincidunt. Suspendisse arcu.

### A.1.1 Lorem 15–17

Nulla in ipsum. Praesent eros nulla, congue vitae, euismod ut, commodo a, wisi. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aenean nonummy magna non leo. Sed felis erat, ullamcorper in, dictum non, ultricies ut, lectus. Proin vel arcu a odio lobortis euismod. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Proin ut est. Aliquam odio. Pellentesque massa turpis, cursus eu, euismod nec, tempor congue, nulla. Duis viverra gravida mauris. Cras tincidunt. Curabitur eros ligula, varius ut, pulvinar in, cursus faucibus, augue.

Nulla mattis luctus nulla. Duis commodo velit at leo. Aliquam vulputate magna et leo. Nam vestibulum ullamcorper leo. Vestibulum condimentum rutrum mauris. Donec id mauris. Morbi molestie justo et pede. Vivamus eget turpis sed nisl cursus tempor. Curabitur mollis sapien condimentum nunc. In wisi nisl, malesuada at, dignissim sit amet, lobortis in, odio. Aenean consequat arcu a ante. Pellentesque porta elit sit amet orci. Etiam at turpis nec elit ultricies imperdiet. Nulla facilisi.

In hac habitasse platea dictumst. Suspendisse viverra aliquam risus. Nullam pede justo, molestie nonummy, scelerisque eu, facilisis vel, arcu.

Curabitur tellus magna, porttitor a, commodo a, commodo in, tortor. Donec interdum. Praesent scelerisque. Maecenas posuere sodales odio. Vivamus metus lacus, varius quis, imperdiet quis, rhoncus a, turpis. Etiam ligula arcu, elementum a, venenatis quis, sollicitudin sed, metus. Donec nunc pede, tincidunt in, venenatis vitae, faucibus vel, nibh. Pellentesque wisi. Nullam malesuada. Morbi ut tellus ut pede tincidunt porta. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam congue neque id dolor.

### A.1.2 Lorem 18–19

Donec et nisl at wisi luctus bibendum. Nam interdum tellus ac libero. Sed sem justo, laoreet vitae, fringilla at, adipiscing ut, nibh. Maecenas non sem quis tortor eleifend fermentum. Etiam id tortor ac mauris porta vulputate. Integer porta neque vitae massa. Maecenas tempus libero a libero posuere dictum. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aenean quis mauris sed elit commodo placerat. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Vivamus rhoncus tincidunt libero. Etiam elementum pretium justo. Vivamus est. Morbi a tellus eget pede tristique commodo. Nulla nisl. Vestibulum sed nisl eu sapien cursus rutrum.

Nulla non mauris vitae wisi posuere convallis. Sed eu nulla nec eros scelerisque pharetra. Nullam varius. Etiam dignissim elementum metus. Vestibulum faucibus, metus sit amet mattis rhoncus, sapien dui laoreet odio, nec ultricies nibh augue a enim. Fusce in ligula. Quisque at magna et nulla commodo consequat. Proin accumsan imperdiet sem. Nunc porta. Donec feugiat mi at justo. Phasellus facilisis ipsum quis ante. In ac elit eget ipsum pharetra faucibus. Maecenas viverra nulla in massa.

## A.2 Lorem 51

Maecenas dui. Aliquam volutpat auctor lorem. Cras placerat est vitae lectus. Curabitur massa lectus, rutrum euismod, dignissim ut, dapibus a, odio. Ut eros erat, vulputate ut, interdum non, porta eu, erat. Cras fermentum, felis in porta congue, velit leo facilisis odio, vitae consectetuer lorem quam vitae orci. Sed ultrices, pede eu placerat auctor, ante ligula rutrum tellus, vel posuere nibh lacus nec nibh. Maecenas laoreet dolor at enim. Donec molestie dolor nec metus. Vestibulum libero. Sed quis erat. Sed tristique. Duis pede leo, fermentum quis, consectetuer eget, vulputate sit amet, erat.

# Appendix B

# The Last Appendix

Appendices are numbered with letters, but the sections and subsections use arabic numerals, as can be seen below.

## B.1 Lorem 20-24

Nulla ac nisl. Nullam urna nulla, ullamcorper in, interdum sit amet, gravida ut, risus. Aenean ac enim. In luctus. Phasellus eu quam vitae turpis viverra pellentesque. Duis feugiat felis ut enim. Phasellus pharetra, sem id porttitor sodales, magna nunc aliquet nibh, nec blandit nisl mauris at pede. Suspendisse risus risus, lobortis eget, semper at, imperdiet sit amet, quam. Quisque scelerisque dapibus nibh. Nam enim. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Nunc ut metus. Ut metus justo, auctor at, ultrices eu, sagittis ut, purus. Aliquam aliquam.

Etiam pede massa, dapibus vitae, rhoncus in, placerat posuere, odio. Vestibulum luctus commodo lacus. Morbi lacus dui, tempor sed, euismod eget, condimentum at, tortor. Phasellus aliquet odio ac lacus tempor faucibus. Praesent sed sem. Praesent iaculis. Cras rhoncus tellus sed justo ullamcorper sagittis. Donec quis orci. Sed ut tortor quis tellus euismod tincidunt. Suspendisse congue nisl eu elit. Aliquam tortor diam, tempus id, tristique eget, sodales vel, nulla. Praesent tellus mi, condimentum sed, viverra at, consectetuer quis, lectus. In auctor vehicula orci. Sed pede sapien, euismod in, suscipit in, pharetra placerat, metus. Vivamus commodo dui non odio. Donec et felis.

Etiam suscipit aliquam arcu. Aliquam sit amet est ac purus bibendum congue. Sed in eros. Morbi non orci. Pellentesque mattis lacinia elit. Fusce molestie velit in ligula. Nullam et orci vitae nibh vulputate auctor. Aliquam eget purus. Nulla auctor wisi sed ipsum. Morbi porttitor tellus ac enim. Fusce ornare. Proin ipsum enim, tincidunt in, ornare venenatis, molestie a, augue. Donec vel pede in lacus sagittis porta. Sed hendrerit ipsum quis nisl. Suspendisse quis massa ac nibh pretium cursus. Sed sodales. Nam eu neque quis pede dignissim ornare. Maecenas eu purus ac urna tincidunt congue.

Donec et nisl id sapien blandit mattis. Aenean dictum odio sit amet risus. Morbi purus. Nulla a est sit amet purus venenatis iaculis. Vivamus viverra purus vel magna. Donec in justo sed odio malesuada dapibus. Nunc ultrices aliquam nunc. Vivamus facilisis pellentesque velit. Nulla nunc velit, vulputate dapibus, vulputate id, mattis ac, justo. Nam mattis elit dapibus purus. Quisque enim risus, congue non, elementum ut, mattis quis, sem. Quisque elit.

Maecenas non massa. Vestibulum pharetra nulla at lorem. Duis quis quam id lacus dapibus interdum. Nulla lorem. Donec ut ante quis dolor bibendum condimentum. Etiam egestas tortor vitae lacus. Praesent cursus. Mauris bibendum pede at elit. Morbi et felis a lectus interdum facilisis. Sed suscipit gravida turpis. Nulla at lectus. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Praesent nonummy luctus nibh. Proin turpis nunc, congue eu, egestas ut, fringilla at, tellus. In hac habitasse platea dictumst.

## B.2 Lorem 25-27

Vivamus eu tellus sed tellus consequat suscipit. Nam orci orci, malesuada id, gravida nec, ultricies vitae, erat. Donec risus turpis, luctus sit amet, interdum quis, porta sed, ipsum. Suspendisse condimentum, tortor at egestas posuere, neque metus tempor orci, et tincidunt urna nunc a purus. Sed facilisis blandit tellus. Nunc risus sem, suscipit nec, eleifend quis, cursus quis, libero. Curabitur et dolor. Sed vitae sem. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Maecenas ante. Duis ullamcorper enim. Donec tristique enim eu leo. Nullam molestie elit eu dolor. Nullam bibendum, turpis vitae tristique gravida, quam sapien tempor lectus, quis pretium tellus purus ac quam. Nulla facilisi.

Duis aliquet dui in est. Donec eget est. Nunc lectus odio, varius at, fermentum in, accumsan non, enim. Aliquam erat volutpat. Proin sit amet nulla ut eros consectetuer cursus. Phasellus dapibus aliquam justo. Nunc laoreet. Donec consequat placerat magna. Duis pretium tincidunt justo. Sed sollicitudin vestibulum quam. Nam quis ligula. Vivamus at metus. Etiam imperdiet imperdiet pede. Aenean turpis. Fusce augue velit, scelerisque sollicitudin, dictum vitae, tempor et, pede. Donec wisi sapien, feugiat in, fermentum ut, sollicitudin adipiscing, metus.

Donec vel nibh ut felis consectetuer laoreet. Donec pede. Sed id quam id wisi laoreet suscipit. Nulla lectus dolor, aliquam ac, fringilla eget, mollis ut, orci. In pellentesque justo in ligula. Maecenas turpis. Donec eleifend leo at felis tincidunt consequat. Aenean turpis metus, malesuada sed, condimentum sit amet, auctor a, wisi. Pellentesque sapien elit, bibendum ac, posuere et, congue eu, felis. Vestibulum mattis libero quis metus scelerisque ultrices. Sed purus.

# Bibliography

[1] H. Chen, K. Laine, R. Player, and Y. Xia. High-precision arithmetic in homomorphic encryption. In *Topics in Cryptology – CT-RSA 2018*, Lecture Notes in Computer Science, pages 116–136. Springer, Mar. 2018. International Conference on Cryptographers Track at the RSA Conference on Topics in Cryptology, CT-RSA 2018 ; Conference date: 16-04-2018 Through 20-04-2018.

[2] C. Christian, M. Silviio, and S. Markus. Computationally private information retrieval with polylogarithmic communication. In J. Stern, editor, *Advances in Cryptology — EUROCRYPT '99: International Conference on the Theory and Application of Cryptographic Techniques*, volume 1592 of *Lecture Notes in Computer Science*, pages 202–214, Prague, Czech Republic, 1999. Springer.

[3] R. Geelen and F. Vercauteren. Bootstrapping for bgv and bfv revisited. *Journal of Cryptology*, 36(12), 2024.

[4] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing. Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In M. F. Balcan and K. Q. Weinberger, editors, *Proceedings of The 33rd International Conference on Machine Learning*, volume 48 of *Proceedings of Machine Learning Research*, pages 201–210, New York, USA, 20–22 Jun 2016. PMLR.

[5] Ilaria Chillotti. TFHE Deep Dive - Ilaria Chillotti, FHE.org, Aug. 2022. YouTube video.

[6] N. J. Bouman. Comparison of Privacy Enhancing Technologies and MPC, Aug. 2024.

[7] A. Kim, Y. Polyakov, and V. Zucca. Revisiting homomorphic encryption schemes for finite fields. In *Lecture Notes in Computer Science*, volume 1309, pages 608–639. Springer, 2021.

[8] S. Klabnik, C. Nichols, and C. Krycho. *The Rust Programming Language*. No Starch Press, 2019. https://doc.rust-lang.org/book/, Accessed: 2025-11-14.

[9] E. Kushilevitz and R. Ostrovsky. Replication is not needed: Single database, computationally-private information retrieval. In *Proceedings of the 38th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 364–373, 1997.

[10] Machine Learning Research. Combining machine learning and homomorphic encryption in the apple ecosystem. URL: `https://machinelearning.apple.com/research/homomorphic-encryption`, last checked on 2025-27-10.

[11] U. Mattsson. Security and Performance of Homomorphic Encryption, Apr. 2025.

[12] S. Pohmann. Personal website. `https://feanortheelf.github.io/personal-website`. Accessed: 2025-11-14.

[13] R. Sion and B. Carbunar. On the computational practicality of private information retrieval. In *Proceedings of the Network and Distributed Systems Security Symposium (NDSS)*, pages 364–373, San Diego, California, USA, 2007. Internet Society (ISOC).

[14] N. P. Smart and F. Vercauteren. Fully homomorphic simd operations. *Designs, Codes and Cryptography*, 71:57 – 81, 2012.