Master's Qualification Exam

Candidate: Laura Viglioni
Supervisor: Prof. Dr. Ricardo Dahab

March 12, 2021

Abstract

lorem ipsum

1 Introduction

escrever sobre como é usado em cripto, qual é nossa motivaçao, lattices sao quentes, problemas de eficiencia, segurança, alternativa nova

Motivation

Summary of objectives

Organization of this document

2 Mathematical background

2.1 Preliminaries

In this text we will consider the Natural Numbers $\mathbb{N}$ the set of all positive integers: $\mathbb{N} = \{1, 2, 3, \dots\}$ and $\mathbb{P}$ the set of all prime numbers.

2.2 Groups

Definition 2.1. A **group** is a set G closed under a binary operation $\cdot$ defined on G such that:

- **Associativity:** $\forall a, b, c \in G,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- **Identity element:** $\exists e \in G\ ;\ \forall a \in G,\ a \cdot e = e \cdot a = a$
- **Inverse element:** $\forall a \in G,\ \exists b \in G\ ;\ a \cdot b = b \cdot a = e$

And it is denoted by $\langle G, \cdot \rangle$, or simply G if the operation is implied.

Definition 2.2. A group is said to be **commutative** or **abelian** if $\forall a, b \in G,\ a \cdot b = b \cdot a$

A group is called **additive** or **multiplicative** if its operation is addition or multiplication, respectively.

Definition 2.3. A subset H of G is a **subgroup** of $\langle G, \cdot \rangle$ if it is closed under $\cdot$ induced by $\langle G, \cdot \rangle$. The **trivial subgroup** of any group is the set consisting of just the identity element.

Definition 2.4. The **order** of a group $\langle G, \cdot \rangle$ is the cardinality of the set G.

Definition 2.5. A subgroup H of G can be used to decompose G in uniform sized and disjoints subsets called **cosets**. Given an element $g \in G$:

- A **left coset** is defined by $gH := \{g \cdot h\ ;\ h \in H\}$
- A **right coset** is defined by $Hg := \{h \cdot g\ ;\ h \in H\}$

2.3 Rings and fields

Definition 2.6. A **ring** is a set together with two binary operations, we will note by $+$ and $*$ and call it addition and multiplication, respectively, such that:

- $\langle R, +\rangle$ is an abelian group.
- $*$ is associative
- $*$ is distributive over $+$

And it is denoted by $\langle R, +, *\rangle$, or simply G if the operations are implied.

Definition 2.7. A ring is said to be **commutative** if its $*$ operation is commutative.

Definition 2.8. A ring is said to be **with unity** if $*$ has a identity element. We shall note it by 1 and it is called **unity**.

Definition 2.9. A **division ring** is a ring R where $\forall r \in R,\ \exists s \in R\ ;\ r * s = 1$.

Definition 2.10. A **field** is a commutative division ring.

2.4 Number fields

Definition 2.11. Let K and L be two fields, L is said to be a **field extension** of K if $L \subseteq K$ and we denote it by L/K

Note that in a field extension L/K, L has a structure of a vector space over K, where vector addition is in L and scalar multiplication $a \in K,\ v \in L \implies av \in L$. The dimension of L as a vector space is called **degree** and it is denoted by $[L : K]$.

Definition 2.12. A field extension is called **number field** when it is over $\mathbb{Q}$.

Definition 2.13. Let $\alpha \in L$ where L/K is a field extension. We say that α is **algebraic over** K if $\exists p \in K[X]\ ;\ p(\alpha) = 0$. p is said to be **the minimal polynomial of** α **over** K denoted by p_α. If $\alpha \in L = \mathbb{Q}[\theta]$, we simply call α an **algebraic number**.

Example 2.1. It is known that $\mathbb{Q}$ is a field. If we add $\sqrt{2}$ to the set, we can build a new field adding also all the powers and multiples of $\mathbb{Q}$. This new field is denoted by $\mathbb{Q}[\sqrt{2}]$, note that $\sqrt{2}$ is algebraic and its minimal polynomial $p_{\sqrt{2}} = x^2 - 2$. All elements of $\mathbb{Q}[\sqrt{2}]$ are in the form $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ and one of its basis is $\{1, \sqrt{2}\}$, so it has degree is 2.

Example 2.2. If we add $\sqrt[3]{2}$ to $\mathbb{Q}$ instead, its elements would have the form $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$, so one of its basis is $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, $p_\alpha = x^3 - 2$ and its degree is 3.

Example 2.3 ([4], Cyclotomic number field)**.** A number field of particular interest is $\mathbb{Q}(\zeta_m)$, the m-th cyclotomic field, where $\zeta_m = \exp 2\pi i/m$ is a primitive m-th root of unity for any integer number $m \geq 1$. The degree of $\mathbb{Q}(\zeta_m)$ is $\phi(m)$, where $\phi(\cdot)$ denotes the Euler's totient function. The minimal polynomial of ζ_m, called the m-th cyclotomic polynomial, is $\Phi_m(x) = \prod_{k \in \mathbb{Z}_m^*}$, where $\mathbb{Z}_m^*$ denotes the group of invertible elements in $\mathbb{Z}/m\mathbb{Z}$.

Example 2.4 ([4], Maximal real subfield)**.** The number field $\mathbb{Q}(\zeta_m + \zeta_m^{-1}) \subset \mathbb{R} \cap \mathbb{Q}(\zeta_m)$ is the maximal real subfield of $\mathbb{Q}(\zeta_m)$ and has degree $\phi(m)/2$ if $m \geq 3$.

Theorem 2.1 ([7], p.40)**.** *If K is a number field, then $K = \mathbb{Q}[\theta]$ for some algebraic number $\theta \in K$, called primitive element.*

Then we conclude that $\{1, \theta, \theta^2, ..., \theta^{n-1}\}$ is a basis for the vector space $K = \mathbb{Q}[\theta]$ over $\mathbb{Q}$. Note that we can represent an number $a \in K$ as a linear combination of θ, *i.e* $a = \sum_{i=0}^{n} a_i\theta^i$ or as a polynomial $a(x) = \sum_{i=0}^{n} a_i x^i$.

Definition 2.14. A number α is said to be an **algebraic integer** if $p \in \mathbb{Z}[X]$; $p(\alpha) = 0$. The set of all algebraic integers of K forms a ring called **ring of integers** of K and is denoted by $\mathcal{O}_K$.

Definition 2.15. An **integral basis** is a basis for a ring of integers.

Definition 2.16 ([5], Section 2.3.2)**.** An **integral Ideal** $\mathfrak{I} \subset \mathcal{O}_K$ is a nontrivial additive subgroup that is also closed under multiplication by $\mathcal{O}_K$, *i.e.*, $r \cdot a \in \mathfrak{I}$ for any $r \in \mathcal{O}_K$ and $a \in \mathfrak{I}$. Any ideal $\mathfrak{I}$ is a free $\mathbb{Z}$-module of rank n, *i.e.*, it is the set off all $\mathbb{Z}$-linear combinations of some basis $\{b_1, \ldots, b_n\} \subset \mathfrak{I}$ of linearly independents (over $\mathbb{Z}$) elements b_i.

Definition 2.17 ([5], Section 2.3.2)**.** A **fractional ideal** $\mathfrak{I} \subset K$ is a set such that $d\mathfrak{I} \subset \mathcal{O}_K$ is an integral ideal for some $d \in \mathcal{O}_K$

Definition 2.18 ([5], Section 2.3.3)**.** For any fractional ideal $\mathfrak{I} \subset K$, its **dual ideal** is defined as $\mathfrak{I}^v := \{a \in K \ ; \ Tr(a\mathfrak{I}) \subset \mathbb{Z}\}$. An important canonical fractional ideal in a number field K is the **codifferent ideal** $\mathcal{O}_K^v$, *i.e.*, the dual ideal of the ring of integers: $\mathcal{O}_K^v := \{a \in K \ ; \ Tr(a\mathfrak{I}) \subset \mathcal{O}_K\}$.

Definition 2.19 (Fixed field by involution)**.** A map $f : K \to K$, where K is a number field, is called **involution** of K if $\forall a, b \in K$ $f(a+b) = f(a)+f(b)$ $f(a \cdot b) = f(a) \cdot f(b)$ and $f(f(a)) = a$. The subfield $F = \{a \in K \ f(a) = a\}$ is called **fixed field by involution** of K.

2.5 The inner product space *H*

Definition 2.20. Let $r, s, n \in \mathbb{Z}_+$ such that $n = r + 2s > 0$. The space $H \subset \mathbb{C}^n$ is defined as:

$$H = \{(a_1, \ldots, a_r, b_1, \ldots, b_s, \overline{b_1}, \ldots, \overline{b_s}) \in \mathbb{C}^n\}$$

where $a_i \in \mathbb{R}$, $\forall i \in \{1, \ldots, r\}$ and $b_j \in \mathbb{C}\backslash\mathbb{R}$, $j \in \{1, \ldots, s\}$. For all $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in H$ the space H is endowed with inner product $\langle x, y \rangle_H$ defined as:

$$\langle x, y \rangle_H = \sum_{i=1}^{n} x_i \overline{y_i} = \sum_{i=1}^{r} x_i \overline{y_i} + \sum_{i=1}^{s} x_{i+r} \overline{y_{i+r}} + \sum_{i=1}^{s} \overline{x_{i+r}} y_{i+r}$$

The ℓ_2-norm and infinity norm of any $x \in H$ are defined as $\|x\| = \sqrt{\langle x, x \rangle_H}$ and $\|x\|_\infty = \max\{|x_i|\}_{i=1}^n$.

It can be proven that H and $\mathbb{R}^n$ are isomorphic.

2.6 Lattices

2.6.1 Basic definitions

Definition 2.21. A Lattice $\Lambda \subset \mathbb{R}^n$ is a subgroup of the additive group $\mathbb{R}^n$

In other words, given m linear independent vectors in $\mathbb{R}^n$, the set $\{v_1, v_2, ..., v_m\}$ is called a **basis** for Λ and the Lattice may defined by:

Definition 2.22.

$$\Lambda := \left\{ x = \sum_{i=1}^{m} \lambda_i v_i \in \mathbb{R}^n \mid \lambda_i \in \mathbb{Z} \right\}$$

I.e., any $\lambda \in \Lambda$ can be written as $\lambda = Mv$ where M is the **generator matrix** of Λ where each row is a vector from the basis and $v \in \mathbb{Z}^n$.

Since the space H (2.20) is isomorphic to $\mathbb{R}^n$, all definitions above can be switched from $\mathbb{R}^n$ to H without any loss of generality.

Definition 2.23. The **minimum distance** of an Lattice Λ is the shortest nonzero vector from Λ, given some norm, *i.e.*:

$$\lambda_1(\Lambda) := \min_{0 \neq v \in \Lambda} \|v\|$$

We define λ_m as the set of $m \in \mathbb{N}$ linear independent vectors of Λ such that the biggest vector from λ_m is equal or smaller than the biggest vector of any linear independent set of length m in Λ. We usually use λ_n, where n is the size of the basis of Λ and we call them **shortest independent vectors** of Λ.

Definition 2.24. Let Λ be a lattice and M its generator matrix. The matrix $G = MM^T$ is called **Gram matrix** for Λ.

2.6.2 Lattice problems

Definition 2.25 ([5], Definition 2.8, Gap Shortest Vector Problem)**.** For an approximation factor $\gamma = \gamma(n) \geq 1$, the $GapSVP_\gamma$ is: given a lattice Λ and length $d > 0$, output **YES** if $\lambda_1(\Lambda) \leq d$ and **NO** if $\lambda_1(L) > \gamma d$.

Definition 2.26 ([5], Definition 2.8, Shortest Independent Vectors Problem)**.** For an approximation factor $\gamma = \gamma(n) \geq 1$, the $SIVP_\gamma$ is: given a lattice Λ, output n linearly independent lattice vectors of length at most $\gamma(n) \cdot \lambda_n(\Lambda)$.

2.7 Learning problems

I this section we will describe some problems that are believed to be hard and used in cryptography.

2.7.1 Learning from Parity

Definition 2.27. Given m vectors uniformly chosen $a_i \leftarrow \mathbb{Z}_2^n$ and some $\epsilon \in [0,1]$, we define the problem **Learn With Parity (LWP)** as:

find $s \in \mathbb{Z}_2^n$ such that for $i \in \{1, \ldots, m\}$

$$\langle s, a_i \rangle \ \approx_\epsilon \ b_i \ \ (mod\, 2)$$

In other words, the equality holds with probability $1 - \epsilon$

2.7.2 Learning with Errors

Definition 2.28. Learning With Errors (LWE) is a generalization of LFP (2.27) with two new parameters $p \in \mathbb{P}$ and χ a probability distribution on $\mathbb{Z}_p$ so that we have:

$$< s, a_i > \approx_\chi \ b_i \ \ (mod\, p)$$

or

$$< s, a_i > + e_i \ = \ b_i \ \ (mod\, p)$$

Where $a_i \leftarrow \mathbb{Z}_p^n$ uniformly and $e_i \leftarrow \mathbb{Z}$ according to χ

Theorem 2.2 ([6], Theorem 1.1)**.** *Let n, p be integers and $\alpha \in (0,1)$ be such that $\alpha p > 2\sqrt{n}$. If there exists an efficient algorithm that solves $LWE_{p\Psi_\alpha}$ then there exists an efficient quantum algorithm that approximates the decision version of the shortest vector problem (GAP_{SVP} 2.25) and the shortest independent vectors problem (SIVP 2.26) to within $\tilde{O}(n/\alpha)$ in the worst case.*

Where Ψ_β is defined as:

$$\forall r \in [0,1), \ \Psi_\beta(r) := \sum_{k=-\infty}^{\infty} \frac{1}{\beta}.\exp\left(-\pi\left(\frac{r-k}{\beta}\right)^2\right)$$

2.7.3 Ring-LWE

Let K be a number field, $R = \mathcal{O}_K$ its ring of integers and $R^\vee$ the codifferent ideal of K. Let $2 \leq q \in \mathbb{N}$ and for any fractional ideal $\mathfrak{I} \subset K$. Also let $K_\mathbb{R}$ be the tensor product $K \otimes_\mathbb{Q} \mathbb{R}$, $\mathfrak{I}_q = \mathfrak{I}/q\mathfrak{I}$ and $\mathbb{T} = K_\mathbb{R}/R^\vee$.

The twisted embeddings can be extended from K to $K_\mathbb{R}$ as follows [[4], Section 3]: for any totally positive $\tau \in F$, the $\mathbb{R}$-vector space $\sigma_\tau(K_\mathbb{R})$ is isomorphic to $H \simeq \mathbb{R}^n$. Consider the extension of the trace function $Tr_K : K \to \mathbb{Q}$ to $Tr_K : K_\mathbb{R} \to \mathbb{R}$, for any $\tau \in F$ totally positive integer we can define the inner product as:

$$\langle a, b \rangle_\tau := \langle \sigma_\tau(a), \sigma_\tau(b) \rangle_H = Tr_K(\tau a \bar{b}), \ \ a, b \in K_\mathbb{R}$$

By considering the inner product $\langle a, b \rangle_\tau$, the $\mathbb{R}$-vector space $K_\mathbb{R}$ is an Euclidian vector space of dimention n isometric to both $(H, \langle a, b \rangle_H)$ and $(\mathbb{R}, \langle a, b \rangle)$.

Definition 2.29 ([5], Definition 2.15, Ring-LWE Average-Case Decision)**.** Let Υ be a distribution over a family of error distributions over $K_\mathbb{R}$. The average-case Ring-LWE decision problem, denoted $R{-}LWEq, \Upsilon$, is to distinguish (with non-negligible advantage) between independent samples from $A_{s,\psi}$ for a *random* choice of $(s, \psi) \longleftarrow U(R_q^\vee) \times \Upsilon$, and the same number of uniformly random and independent samples from $R_q \times \mathbb{T}$.

Theorem 2.3 ([5], Corollary 5.2)**.** *Let $\alpha = \alpha(n) \in (0,1)$, and let $q = q(n)$ be an integer such that $\alpha q \geq 2\sqrt{n}$. Then, there is* a polynomial-time quantum reduction from *$SIVP_{\gamma'}$ and $GapSVP_{\gamma'}$* to (average-case, decision) *$LWE_{q,\alpha}$.*

Definition 2.30 ([2], Definition 3.2, Ring-LWE Search)**.** Let Ψ be a family of distributions over $K_{\mathbb{R}}$. The search version of the $ring - LWE$ problem, denoted $R - LWE_{q,\Psi}$, is defined as follows: given access to arbitrarily many independent samples from $A_{s,\psi}$ for some arbitrary $s \in R_q^{\vee}$ and $\psi \in \Psi$, find s.

Theorem 2.4 ([2], Theorem 3.6)**.** *Let K be the mth cyclotomic number field having dimension $n = \phi(m)$ and $R = \mathcal{O}_K$ be its ring of integers. Let $\alpha < \sqrt{(\log n)/n}$, and let $q = q(n) \geq 2$, $q = 1 \ (mod\ m)$ be a $poly(n)$-bounded prime such that $\alpha q \geq \omega(\sqrt{\log n})$. Then there is a polynomial-time quantum reduction from $\tilde{O}(n/\alpha)$-approximate $SIVP$ (or SVP) on ideal lattices in K to $R - DLWE_{q,\Upsilon_\alpha}$. Alternatively, for any $l \geq 1$, we can replace the target problem by the problem of solving $R - DLWE_{q,D_\xi}$ given only l samples, where $\xi = \alpha \cdot (nl/\log{(nl)})^{1/4}$*

2.8 Twisted Embeddings

2.8.1 Embeddings

Definition 2.31. Let K and L be two field extensions and a homomorphism $\phi : K \to L$. ϕ is said to be a **$\mathbb{Q}$-homomorphism** if $\phi(a) = a, ; \forall a \in \mathbb{Q}$

Definition 2.32. A $\mathbb{Q} - homomorphism; \phi : K \to \mathbb{C}$ is called an **embedding**.

Theorem 2.5 ([7], p.41)**.** *If K is a number field with degree n then there are exactly n embeddings $\sigma_i : K \to \mathbb{C}$ where by $\sigma_i(\theta) = \theta_i$ where $\theta_i \in \mathbb{C}$ is a distinct zero of the K's minimum polynomial.*

Definition 2.33 (Trace and Norm)**.** Let $x \in K$ be an element of a number field and $\{\sigma_i\}_{i=1}^n$ the possible embeddings. The elements $\{\sigma_i(x)\}_{i=1}^n$ are called **conjugates** of x and we define the **norm** of x $N(x)$ and **Trace** of x $Tr(x)$ respectively:

$$N(x) = \prod_{i=1}^{n} \sigma_i(x) \ , \ Tr(x) = \sum_{i=1}^{n} \sigma_i(x)$$

Theorem 2.6 ([7], p.54)**.** *For any $x \in K$, we have $N(x), Tr(x) \in \mathbb{Q}$. If $x \in \mathcal{O}_K$, we have $N(x), Tr(x) \in \mathbb{Z}$.*

Definition 2.34. Let $\{\sigma_i\}_n$ the possible embeddings of a number field K. Let r the number of embeddings with real images and $2s$ the complex ones, then $r + 2s = n$. The pair (r, s) is called **signature** of K.

Definition 2.35. The homomorphism $\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s$, where (r, s) is the signature of K, is said to be the **canonical embedding** and is defined by:

$$\sigma(x) = (\sigma_1(x), ..., \sigma_r(x), \sigma_{r+1}(x), ..., \sigma_{r+s}(x))$$

Note that we could rewrite the canonical embedding as $\sigma : K \to \mathbb{R}^n$

$$\sigma(x) = (\sigma_1(x), ..., \sigma_r(x), \Re(\sigma_{r+1}(x)), \Im(\sigma_{r+1}(x)), ..., \Re(\sigma_{r+s}(x)), \Im(\sigma_{r+s}(x)))$$

For now on we will denote it simply by:

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_r(x), \sigma_{r+1}(x), \ldots, \sigma_{r+2s}(x))$$

2.8.2 Algebraic lattices

Theorem 2.7 ([7], p.155)**.** *Let $\{\omega_1, ..., \omega_n\}$ be an integral basis of K, The n vectors $v_i = \sigma(\omega_i) \in \mathbb{R}^n$ are linearly independent, so they define a full rank algebraic lattice $\Lambda = \Lambda(\mathcal{O}_K) = \sigma(\mathcal{O}_K)$.*

The generator matrix of $\Lambda = \sigma(\mathcal{O}_K)$ is defined by:

$$\begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_{r+2s}(\omega_1) \\ & \vdots & \\ \sigma_1(\omega_n) & \ldots & \sigma_{r+2s}(\omega_n) \end{pmatrix} \tag{1}$$

Remark 2.1. An embedding creates the correspondence between a point $\lambda \in \Lambda \subset \mathbb{R}^n$ of an algebraic lattice (Theo. 2.7) and an integer in $\mathcal{O}_K$:

Let λ be a point of a lattice Λ:

$$\begin{aligned} \lambda &= (\lambda_1, \ldots, \lambda_{r+2s}) \in \Lambda \\ &= \left(\sum_{i=1}^{n} z_i \sigma_1(\omega_i), \ldots, \sum_{i=1}^{n} z_i \sigma_{r+2s}(\omega_i) \right) \\ &= \left(\sigma_1 \left(\sum_{i=1}^{n} z_i \omega_i \right), \ldots, \sigma_{r+2s} \left(\sum_{i=1}^{n} z_i \omega_i \right) \right) \end{aligned}$$

where $z_i \in \mathbb{Z}$. Since any element $x \in \mathcal{O}_K$ has the form $x = \sum_{i=1}^{n} \lambda_i \omega_i$, we can conclude that:

$$\lambda = (\sigma_1(x), \ldots, \sigma_{r+2s}(x)) = \sigma(x)$$

2.8.3 Twisted embeddings

Definition 2.36. Let K be a number field with degree n and σ an embedding. We say that a number $\tau \in F$, where F is the fixed field by involution of K (Definition 2.19) is **totally positive** if $\forall i \in 1, \ldots, n,\ \sigma_i(\tau) \in \mathbb{R}_+^*$.

Definition 2.37 (Twisted Embedding)**.** Given τ a totally positive number, the **τ-twisted embedding**, or simply twisted embedding, is the monomorphism defined as:

$$\sigma_\tau(x) = (\sqrt{\tau_1}\sigma_1(x), \ldots, \sqrt{\tau_{r+2s}}\sigma_{r+2s}(x))$$

where $\tau_i = \sigma_i(\tau)$.

3 Twisted embeddings and cryptography

3.1 Twisted Ring-LWE

In this section we present variant of the Ring-LWE (Definition~2.30) using twisted embeddings (Definition~2.37).

Definition 3.1 ([4], Twisted Ring-LWE distribution)**.** For a totally positive element $\tau \in F$, let ψ_τ denote an error distribution over the inner product $\langle \cdot, \cdot \rangle_\tau$ and $s \in R_q^\vee$ (the "secret") be an uniformly randomized element. The *Twisted Ring-LWE distribution* $\mathcal{A}_{s,\psi_\tau}$ produces samples of the form

$$(a, b = a \cdot s + e \mod qR^\vee) \in R_q \times K_\mathbb{R}/qR^\vee.$$

Solving the Twisted Ring-LWE is as hard as solving the usual Ring-LWE as stated in Theorem~3.1:

Theorem 3.1 ([4], Theorem 1)**.** *Let K be an arbitrary number field, and let $\tau \in F$ be totally positive. Also, let (s, ψ) be randomly chosen from $(U(R_q^\vee) \times \Psi)$ in $(K_\mathbb{R}, \langle \cdot, \cdot \rangle_{\tau=1})$. Then there is a polynomial-time reduction from $Ring-LWE_{q,\psi}$ to $Ring-LWE^{\tau}_{q,\psi_\tau}$.*

3.2 Error sampling in rotated $\mathbb{Z}^n$-lattices

In this section we present the *Ortiz et al.* ([4], Section 8) variation of the cryptosystem of Lyubashevsky, Peikert, and Regev ([3], Section 8.2) using twisted embeddings. Let R be an m-th cyclotomic ring and $p, q \in \mathbb{Z}$ coprimes. The message space is defined as R_p and it is required q to be coprime with every odd prime dividing m. Consider that ϕ_τ is an error distribution over $(K_\mathbb{R}, \langle \cdot, \cdot \rangle_\tau)$ and $\lfloor \cdot \rceil$ denotes a valid discretization to (cosets) of $R^\vee$ or $pR^\vee$. Also, $\hat{m} = m/2$ if m is even, otherwise $\hat{m} = m$. Finally, for any $\overline{a} \in \mathbb{Z}_q$, let $[[\overline{a}]]$ denote the unique representative $a \in (\overline{a} + q\mathbb{Z}) \cap [-q/2, q/2)$, which is entry-wise extended to polynomials.

- **Key generation**: choose a uniformly random $a \in R_q$. Choose $x \longleftarrow \lfloor \phi_\tau \rceil$ and $e \longleftarrow \lfloor p \cdot \phi_\tau \rceil_{pR^\vee}$. Output $(a, b = \hat{m} \cdot (a \cdot x + e) \mod qR) \in R_q \times R_q$ as the public key and x as the secret key.

- **Encryption**: choose $z \longleftarrow\longleftarrow \lfloor \phi_\tau \rceil_R^\vee$, $e' \longleftarrow \lfloor p \cdot \phi_\tau \rceil_{pR^\vee}$ and $e'' \longleftarrow \lfloor p \cdot \phi_\tau \rceil_{t^{-1}\mu + pR^\vee}$, where $\mu \in R_p$ is the word to be encrypted. Let $u = \hat{m} \cdot (a \cdot z + e') \mod qR$ and $v = z \cdot b + e'' \in R_q^\vee$. Output $(u, v) \in R_q \times R_q^\vee$.

- **Decryption**: Given the encrypted message (u, v), compute $v - u \cdot x \mod qR^\vee$, and decode it to $d = [[v - u \cdot x]] \in R^\vee$. Output $\mu = t \cdot d \mod pR$.

In this cryptosystem, the most expensive operations to compute are the error sampling, its discretization and the polynomial multiplications. When R is the ring of integers of the maximum real subfield (2.4) $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, the sampling of error terms can be performed directly over $(K_\mathbb{R}, \langle \cdot, \cdot \rangle_\tau)$ in the orthonormal basis while preserving the spherical format and standard deviation in respect to the corresponding distribution in H. The efficiency of discrete sampling when $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is reinforced by the fact that the discretization in $\mathbb{Z}^n$-lattices is simply a coordinate-wise rounding to the nearest integer. ([4], Section 8).

3.3 Impacts of the twisted embeddings

The correspondence between a point $\lambda \in \Lambda$ of a lattice and an algebraic integer $x \in \mathcal{O}_K$ of a ring of integers (Remark 2.1), *i.e.*, $\lambda = (\sigma_1(x), \ldots, \sigma_{r+2s}(x)) = \sigma(x)$, where σ is the canonical embedding (Definition 2.35), allow us to sample errors over a Lattice and convert them through the embedding to the polynomial representation, *i.e.*, the representation of an element of a ring of integers.

This conversion is trivial when the Lattices we are dealing are rotations of $\mathbb{Z}^n$, otherwise it can be very expensive. With the canonical embedding (Definition 2.35) we can achieve a $\mathbb{Z}^n$ rotated Lattice with the cyclotomic number field with power of 2 dimension ([2], [1]).

Using the Twisted Embedding (Definition 2.37) we can obtain different lattices from the same number field:

Example 3.1 ([4], Example 3). Let $K = \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3}\ ;\ a, b \in \mathbb{Q}\}$ be a totally real number field with degree 2. It follows that the fixed field by involution $F = K$. For any totally positive element $\tau \in F$, consider the lattice $M_\tau = \mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$ in the inner product space $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$. The set $\{1, \sqrt{3}\}$ in a $\mathbb{Z}$-basis of M_τ and the Gram matrix of the lattice M_τ is given by:

$$G_\tau = \begin{bmatrix} Tr_K(\tau) & Tr_K(\tau\sqrt{3}) \\ Tr_K(\tau\sqrt{3}) & Tr_k(3\tau) \end{bmatrix}$$

For example, for $\tau = 1$ and $\tau = 2 + \sqrt{3}$, the Gram matrices are given by:

$$G_1 = \begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix} \quad \textit{and} \quad G_{2+\sqrt{3}} = \begin{bmatrix} 4 & 6 \\ 6 & 12 \end{bmatrix}$$

It can be shown that these two lattices are not equivalent.

The theorem (Theorem 3.2), proposition (Proposition 3.2.1) and corollary (Corollary 3.2.1) bellow show that we can build $\mathbb{Z}^n$-rotated lattices from the maximal real subfield (Example 2.4) using twisted embeddings, *i.e.*, the errors sampled on these lattices can be trivially converted to polynomial representation as elements of a number field.

Theorem 3.2 ([4], Theorem 5). *Let K be a number field with fixed field by the involution F. Consider $\tau \in F$ totally positive and $\mathfrak{I} \subset \mathcal{O}_K$ a fractional ideal such that $\mathfrak{I}$ is an ideal lattice in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$. If $\mathfrak{I}$ is an orthonormal lattice, then both the format and the standard deviation of a spherical Gaussian distribution in an orthonormal basis of $\mathfrak{I} \subset K_\mathbb{R}$ are preserved when seen in the canonical basis of the space H (via the twisted embedding σ_τ).*

Proposition 3.2.1 ([4], Proposition 2). *Let $p \geq 5$ be a prime number, and let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $\tau = \frac{1}{p}(1 - \zeta_p)(1 - \zeta_p^{-1})$. Then $\mathcal{O}_K$ in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$ is an orthonormal lattice with basis $\mathcal{C}^\perp = \{e'_1, \ldots, e'_n\ ;\ e'_n = e_n$ and $e'_j = e_j + e'_{j+1}\}$ where $\mathcal{C} = \{e_1, \ldots, e_n\}$ is the integral basis of K.*

Corollary 3.2.1 ([4], Corollary 1). *Let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ for $p \geq 5$ prime and let $v \in \mathcal{O}_K$ be a random variable distributed as ψ_s^n in the basis $\mathcal{C}^\perp$. Then, the dstribution of $(T^{-1} \circ \sigma_\tau)(v)$ for $\tau = \frac{1}{p}(1-\zeta_p)(1-\zeta_p^{-1})$, seen in the canonical basis of H, is the spherical Gaussian ψ_s^n.*

These new constructions with a more variety of possible rings increase the security notions of Ring-LWE (Definitions~2.30,~2.29), since specific rings might have specific vulnerabilities, thinking about cryptosystems security, that other rings don't. It's important to remark that each number field has it's own polynomial representation and specifically a polynomial $f(x)$ that defines the ring we use as a parameter in the Ring-LWE cryptosystems. That said, the size of the parameters, therefore keys, encrypted messages etc, and the cost of the Ring-LWE operations depends on the polynomial representation of the ring and of $f(x)$.

There is though an open question if there exist other number fields that we build orthonormal lattices and its polynomial arithmetic are efficiently enough for be used in cryptosystems.

4 Objectives

validar a ideia de twisted embedings em varios aspectos, investigaçao em parte teorica e pratica das hipoteses levantadas no artigo sobre as vantagens de usar o twisted, practical impacts do artigo

5 Methodology

5.1 Literature review

5.2 Activities

- Second semester of 2021
- ...

6 Conclusion

References

[1] Léo Ducas and Alain Durmus. Ring-lwe in polynomial rings. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *Public Key Cryptography – PKC 2012*, pages 34–51, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[2] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6110 LNCS(015848):1–23, 2010.

[3] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-lwe cryptography. Cryptology ePrint Archive, Report 2013/293, 2013. `https://eprint.iacr.org/2013/293`.

[4] Jheyne N. Ortiz, Robson R. de Araujo, Diego F. Aranha, Sueli I. R. Costa, and Ricardo Dahab. The Ring-LWE problem in lattice-based cryptography: in praise of the twisted embeddings. To be published, 2021.

[5] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-LWE for any ring and modulus. *Proceedings of the Annual ACM Symposium on Theory of Computing*, Part F1284:461–473, 2017.

[6] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):1–37, 2009.

[7] Ian Stewart and David Tall. *Algebraic number theory.* A K Peters, 2002.