Universidade Estadual de Campinas
Instituto de Computação

Laura Viglioni

The Dissertation or Thesis Title in English

CAMPINAS
1500

Laura Viglioni

The Dissertation or Thesis Title in English

Dissertação apresentada ao Instituto de Computação da Universidade Estadual de Campinas como parte dos requisitos para a obtenção do título de Mestra em Ciência da Computação.

Dissertation presented to the Institute of Computing of the University of Campinas in partial fulfillment of the requirements for the degree of Master in Computer Science.

Supervisor/Orientador: Prof. Dr. Ricardo Dahab

Este exemplar corresponde à versão da Dissertação entregue à banca antes da defesa.

CAMPINAS
1500

Na versão final esta página será substituída pela ficha catalográfica.

De acordo com o padrão da CCPG: “Quando se tratar de Teses e Dissertações financiadas por agências de fomento, os beneficiados deverão fazer referência ao apoio recebido e inserir esta informação na ficha catalográfica, além do nome da agência, o número do processo pelo qual recebeu o auxílio.”
e
“caso a tese de doutorado seja feita em Cotutela, será necessário informar na ficha catalográfica o fato, a Universidade convenente, o país e o nome do orientador.”

Na versão final, esta página será substituída por outra informando a composição da banca e que a ata de defesa está arquivada pela Unicamp.

Chapter 1

Introduction

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

Chapter 2

Mathematical background

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.

2.1 Groups

Definition 2.1.1. 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 2.1.2. 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 2.1.3. 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 2.1.4. The **order** of a group $\langle G, \cdot \rangle$ is the cardinality of the set G.

Definition 2.1.5. 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 $Hg := \{h \cdot g\ ;\ h \in H\}$

2.2 Rings and fields

Definition 2.2.1. 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 2.2.2. A ring is said to be **commutative** if its $*$ operation is commutative.

Definition 2.2.3. 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 2.2.4. A **division ring** is a ring R where $\forall r \in R,\ \exists s \in R\ ;\ r * s = 1$.

Definition 2.2.5. A **field** is a commutative division ring.

2.3 Number fields

Definition 2.3.1. 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 2.3.2. A field extension is called **number field** when it is over $\mathbb{Q}$.

Definition 2.3.3. 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 2.3.1. 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 2.3.2. 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 2.3.3 ([3], 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 2.3.4 ([3], 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 2.3.1 (add font 45 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 2.3.4. 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 2.3.5. An **integral basis** is a basis for a ring of integers.

Definition 2.3.6 ([4], 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 2.3.7 ([4], Section 2.3.2). A **fractional ideal** $\mathfrak{I} \subset K$ is a set sutch that $d\mathfrak{I} \subset \mathcal{O}_K$ is an integral ideal for some $d \in \mathcal{O}_K$

Definition 2.3.8 ([4], 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 2.3.9 (Foxed field by involution). A map $f : K \to K$, where K is a number field, is callend **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.

2.4 The inner product space *H*

Definition 2.4.1. 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.

2.5 Lattices

2.5.1 Basic definitions

Definition 2.5.1. 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 2.5.2.

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

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

Definition 2.5.3. 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.

2.5.2 Lattice problems

Definition 2.5.4 ([4], 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 2.5.5 ([4], 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 $\gamma(n) \cdot \lambda_n(\Lambda)$.

2.6 Learning problems

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

2.6.1 Learning from Parity

Definition 2.6.1. 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 $1 - \epsilon$

2.6.2 Learning with Errors

Definition 2.6.2. Learning With Erros (LWE) is a generalization of LFP (2.6.1) 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 2.6.1 ([5], 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} 2.5.4) and the shortest independent vectors problem (SIVP 2.5.5) to within $\tilde{O}(n/\alpha)$ in the worst case.*

Where Ψ_β is defined as:

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

2.6.3 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 $\mathfrak{I} \subset K$, let $\mathfrak{I}_q = \mathfrak{I}/q\mathfrak{I}$ and $\mathbb{T} = K_\mathbb{R}/R^\vee$.

Definition 2.6.3 ([4], 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 2.6.2 ([4], 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 2.6.4 ([1], 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 2.6.3 ([1], 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 $\xi = \alpha \cdot (nl/\log{(nl)})^{1/4}$*

2.7 Twisted Embeddings

2.7.1 Embeddings

Definition 2.7.1. 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 2.7.2. A $\mathbb{Q} - homomorphism; \phi : K \to \mathbb{C}$ is callend an **embedding**.

Theorem 2.7.1 (inserir fonte 45, 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 mininum polynomial.*

Definition 2.7.3 (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 2.7.2. *For any $x \in K$, we have $N(x), Tr(x) \in \mathbb{Q}$. If $x \in \mathcal{O}_K$, we have $N(x), Tr(x) \in \mathbb{Z}$.*

inserir referencia 45, p54

Definition 2.7.4. 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 2.7.5. 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:

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

2.7.2 Algebraic lattices

Theorem 2.7.3. *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 thety define a full rank algebraic lattice $\Lambda = \Lambda(\mathcal{O}_K) = \sigma(\mathcal{O}_K)$.*

adiciona citaçao 45, p155

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

$$\begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_{r+2s}(\omega_1) \\ & \vdots & \\ \sigma_1(\omega_n) & \ldots & \sigma_{r+2s}(\omega_n) \end{pmatrix} \tag{2.1}$$

Remark 2.7.1. An embedding creates the correspondence between a point $\lambda \in \Lambda \subset \mathbb{R}^n$ of an algebraic lattice (Theo. 2.7.3) 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:

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

2.7.3 Twisted embeddings

Definition 2.7.6. 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 2.3.9) is **totally positive** if $\forall i \in 1, \ldots, n,\ \sigma_i(\tau) \in \mathbb{R}_+^*$.

Definition 2.7.7 (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 $\tau_i = \sigma_i(\tau)$.

Chapter 3

Twisted embeddings and cryptography

3.1 Twisted Ring-LWE

In this section we present variant of the Ring-LWE (Definition 2.6.4) using twisted embeddings (Definition 2.7.7).

Definition 3.1.1 ([3], 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 3.1.1:

Theorem 3.1.1 ([3], 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 thereis 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.* ([3], Section 8) variation of the cryptosystem of Lyubashevsky, Peikert, and Regev ([2], Section 8.2) using twisted embeddings. Let R be an m-th cyclotomic ring and $p, q \in \mathbb{Z}$ coprimes. The message sapce 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 $\mu = t \cdot d \mod pR$.

Im 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 (2.3.4) $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, the sampling of error terms can be performed directly over $(K_\mathbb{R}, \langle \cdot, \cdot \rangle_T)$ 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. ([3], Section 8).

Chapter 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

Chapter 5

Methodology

5.1 atividades, cronograma

Bibliography

[1] 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.

[2] 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`.

[3] 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.

[4] 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.

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