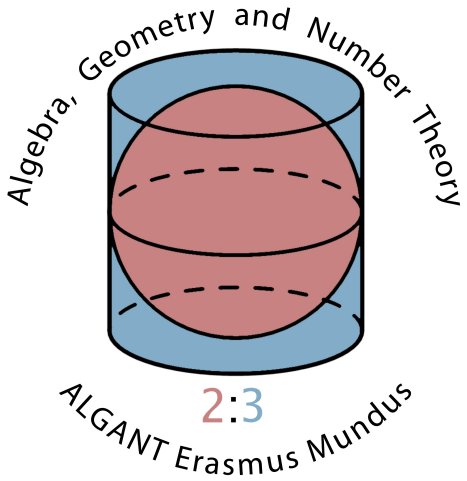

Lattice-Based Cryptography

Federico Bergami

Advised by Prof. Christine Bachoc

Università di Padova

Université de Bordeaux

ALGANT Master's Thesis - 20 July, 2016

Why pure Math [Orl15]

Contents

Acknowledgements

I am very thankful to Prof. Christine Bachoc, who has been very supportive not only during the preparation of this work, but also throughout this year I spent in Bordeaux. Furthermore, I am likewise grateful to all the students and professors I had the chance to meet during these two years, who taught me a different way of doing Mathematics.

A warm thanks goes to my friends back in Bologna: the time spent with you during holidays and breaks has been extremely cheerful and inestimable.

Finally and mostly, I am deeply greatful to my Family and Martina: your enduring support is by far the most invaluable thing I have in my life.

List of Algorithms

List of Figures

Introduction

As the development of actual quantum computers is on the rise day by day, so are concerns about the safety of cryptosystems now being used. Indeed, by exploiting quantum mechanics and its superposition principle, quantum computers store information in *qubits* rather than classical bits. Being a two-state quantum-mechanical system, a qubit does not only have 0 and 1 as possible states since they entail also a superposition of both. Namely, the state of a qubit can be represented as a vector $|\psi\rangle$ in a two dimensional vector space with orthonormal basis $\{|0\rangle, |1\rangle\}$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{with } \alpha, \beta \in \mathbb{C} \quad \text{and } \alpha^2 + \beta^2 = 1$$

The capacity of encoding information in a smaller number of qubits allows quantum computers to outperform classical algorithms in handling many different problems, especially those which require the enumeration of manifold cases. Despite the many doubts cast on the chance of making quantum computers practical, several technical improvements have been recently carried out towards this direction[IBM15, DWA15] and countermeasures are being taken accordingly. For example, NSA openly revealed the plan to shift from current encryption schemes to new ones, yet to be developed, which could resist quantum attacks[NSA15]. As a matter of fact, Shor's factoring algorithm[Sho97] unveiled the vulnerability of many public-key crytography protocols such as RSA, Diffie-Hellman Cryptosystem and ECDH(*Elliptic Curve Diffie-Hellman*), which have turned out to be breakable by quantum algorithms. On the other hand, besides being very hard to solve by using classical algorithms, problems based on lattices are believed to remain diffi-

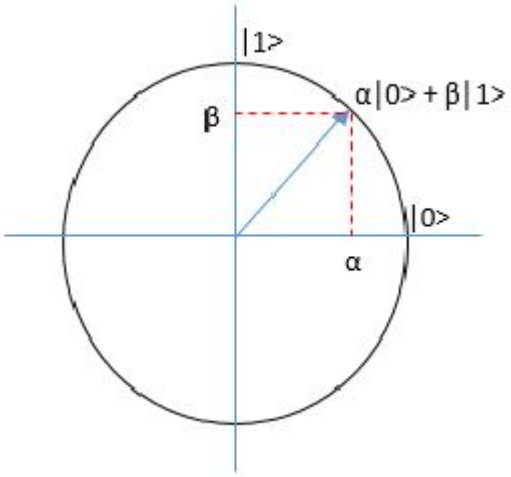

Figure 1: *Representation of the state of a qubit*

cult to tackle also in the quantum setting. This is why, since the development of Ajtai-Dwork cryptosystem and NTRU cryptosystem in the late Ninties, research along this path has been steadily done. However, the **conjectured security against quantum attacks** is not the only reason why great effort is being put in the study of lattice-based cryptosystem.

To name but a few, lattice-based protocols are quite **simple to implement** and **highly parallelizable**: they usually involve only linear operations such as sum or multiplication matrix-vector. Furthermore, these operations are modulo a relatively small integer, usually in the hundreds, so we have a bound for the integers considered .

Secondly, lattice-based cryptosystems usually enjoy strong **security guarantees from worst-case hardness**, which means that breaking their security is proved at least as hard as solving some lattice problems in any of its instances, also the worst ones. This is qualitatively different from the average-case hardness typical of generic cryptographic constructions, which require that random instances, drawn according to a specific probability dis-

tribution, are difficult to solve. The very first example of *worst-case* to *average-case* reduction was done by Ajtai in his pioneering paper [Ajt96a]: he showed that a particular lattice problem is hard on average as long as a related one is hard in the worst case; then he developed an encryption scheme based on the former problem, thus linking the security of his scheme to the possiblity of finding a hard instance of the latter.

Finally, lattices can be used to develop **efficient and adaptable cryptographic tools**. Among them, the most outstanding and longed for is the concept of fully homomorphic encryption, which allows an untrusted worker to manipulate encrypted data in arbitrarily complex ways, without getting any knowledge out of them. After being conceived around thirty years ago by Rivest *et al.*[RAD78], in 2009 this idea was implemented by Gentry, who proposed a solid candidate based on lattices[Gen09a, Gen09b], thus paving the way to further studies [CMNT11, BV12, GSW13].

Outline and Aim

The scope of this thesis is to give a general overview on lattice-based cryptography, discussing its development in the last 20 years and focusing on encryption schemes and hash functions. This presentation is divided into 5 different chapters that we briefly describe.

In **Chapter 1** we introduce the relevant concepts related to lattices that we are going to use and we define many lattice problems together with their complexity. Furthermore, we present some notions of probability that will be needed in the definition of certain lattice problem, namely the Learning with Errors problem.

In **Chapter 2** we describe the first two examples of protocols based on lattices, namely the Ajtai-Dwork Encryption Scheme and the NTRU. In

addition, we discuss their complexity and their practical implementations, underlining their main differences.

In **Chapter 3** we define the Short Integer Solutions(SIS) and the Learning with Errors(LWE) problems, which are the most important average-case lattice problems as far as cryptographic applications are concerned. We outline their main feature and we introduce some basic protocols relying on them, namely various hash functions and an encryption scheme.

In **Chapter 4** we introduce the Ring-Learning with Errors Problem, which is the analogue of LWE in algebraic structured lattices. Here we discuss its main advantages and we focus on its hardness, proving part of the worst-case to average-case reduction which links it to a particular lattice problem.

Finally, in **Chapter 5** we present some of the open problems of lattice-based cryptography stemming from our work.

Notations

We now explain the notations adopted in this present composition.

We will use bold lower-case letters to indicate **vectors** (i.e. $\mathbf{v}$), while bold upper-case letters for **matrices** (i.e. $\mathbf{A}$). Furthermore, the *transposed* of a matrix $\mathbf{A}$ will be denoted by $\mathbf{A}^T$ and given $m \in \mathbb{N}$ we define $[m] = \{1, \dots m\}$ and $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$.

For a vector $\mathbf{x} = (x_1 \dots, x_n) \in \mathbb{R}^n$ or $\mathbb{C}^n$ and $p \in [1, \infty]$, we define the l_p **norm** as $\|\mathbf{x}\|_p = (\sum_{i\in[n]} |x_i|^p)^{1/p}$ when $p < \infty$ and $\|x\|_\infty = \max_{i\in[n]} |x_i|$ when $p = \infty$. When omitted, we will imply $p = 2$. Finally, for a polynomial $f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{R}[x]$, we define $\|f\|_p = (\sum_{i\in[n]} |a_i|^p)^{1/p}$ and $\|f\|_\infty = \max_{i\in[n]} |a_i|$.

As for computational complexity, we use the traditional "**big O notation**". Namely, given two function $f, g : \mathbb{N} \mapsto \mathbb{R}$ we will use the following symbols:

- $f(n) = O(g(n))$ if $\exists\ k > 0$ and $n_0 > 0$ such that $\forall n \geq n_0$, $|f(n)| \leq k \cdot |g(n)|$;
- $f(n) = \Theta(g(n))$ if $\exists\ k_1,\ k_2 > 0$ and $n_0 > 0$ such that $\forall n \geq n_0$, $k_1 \cdot g(n) \leq f(n) \leq k_2 \cdot g(n)$;
- $f(n) = \omega(g(n))$ if $\exists k > 0$ and $n_0 > 0$ such that $\forall n \geq n_0$, $|f(n)| \geq k \cdot |g(n)|$;

- $f(n) = \Omega(g(n))$ if $\exists\ k > 0$ and $n_0 > 0$ such that $\forall n \geq n_0$, $f(n) \geq k \cdot g(n)$.

In addition, we will also use the "Soft-Oh" notation to hide logarithmic factor, i.e. with $O\tilde{(}f)$ we mean $O(f) \times (\log f)^{O(1)}$.

When discussing the security of a cryptographic protocol, we will use the notion of **bits of security**, i.e. a cryptosystem has n bits of security when in average 2^n operations are required to break it.

Finally, given a set of events $\mathcal{B}$ we indicate with $U(\mathcal{B})$ the uniform distribution over $\mathcal{B}$.

Chapter 1

Preliminaries

In this first chapter we introduce the basic notions we are going to use in our paper. First of all, we define lattices, some of their properties and a few of the related concepts. Secondly, we describe lattices problems used in cryptography and discuss the running time of algorithms designed to solve them. Finally, we illustrate some tools of Probability Theory crucial for the definition of the Learning with Errors problem.

1.1 Lattices

1.1.1 Basic Definitions

Definition 1.1 (**Full rank lattice**)**.** An n-dimensional full rank lattice is the set of all integer combinations

$$\{\sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \text{ for } 1 \leq i \leq n\} \tag{1.1}$$

of n linearly independent vectors $\mathbf{b}_1, \cdots, \mathbf{b}_n$ in $\mathbb{R}^n$.

Remark 1. The set $\{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ is called a *basis* for the lattice and it can be represented by the matrix $\mathbf{B} = [\mathbf{b}_1, \cdots, \mathbf{b}_n] \in \mathbb{R}^{n \times n}$ whose columns are the basis vectors. We will denote the lattice generated by $\mathbf{B}$ as $\mathcal{L}(\mathbf{B})$ and we notice that $\mathcal{L}(\mathbf{B}) = \{\mathbf{Bx} : \mathbf{x} \text{ in } \mathbb{Z}\}$ where $\mathbf{Bx}$ is the usual matrix-vector

product. Since we are going to deal only with full rank lattices, from now on we will simply address to them with the term *lattices*.

Definition 1.2 (**Minimum Distance and i-th Successive Minimum**)**.** The minimum distance λ_1 of a lattice $\mathcal{L}$ is the miminum distance between any two distinct lattice points :

$$\lambda_1 = \min\{\text{dist}(\mathbf{x}, \mathbf{y}) : \mathbf{x} \neq \mathbf{y} \in \Lambda\} \tag{1.2}$$

$$= \min\{\|\mathbf{x}\| : \mathbf{x} \in \Lambda\} \tag{1.3}$$

where the second equality comes from the closure of lattices under addition. This definition can be generalized to define the i-th successive minimum λ_i as the smallest $r \in \mathbb{R}$ such that $\mathcal{L}$ has i linearly indepedent vectors of norm at most r.

Definition 1.3 (**Dual Lattice**)**.** The dual lattice of a lattice $\mathcal{L} \in \mathbb{R}^n$ is defined as

$$\mathcal{L}^* := \{\mathbf{w} \in \mathbb{R}^n : \langle \mathbf{w}, \mathcal{L} \rangle\} \subseteq \mathbb{Z} \tag{1.4}$$

i.e., the set of points whose inner products with all the vectors in $\mathcal{L}$ are all integers.

Remark 2. A simple computation shows that $\mathcal{L}^*$ is a lattice. For example, $(\mathbb{Z}^n)^* = \mathbb{Z}^n$ and $(c\mathcal{L})^* = c^{-1}\mathcal{L}^*$ for every $c \in \mathbb{R}$ and different from zero. It is also easy to prove that if $\mathcal{L} = \mathcal{L}(\mathbf{B})$, then $\mathbf{B}^{-T} := (\mathbf{B}^{-1})^T$ is a basis of $\mathcal{L}$.

An important role in lattice-based cryptograhy is played by q-ary lattices, which make up a particular family of lattices in one-to-one correspondance with linear codes in $\mathbb{Z}_q^n$.

Definition 1.4 (**q-ary Lattice**)**.** A lattice $\mathcal{L} \subset \mathbb{Z}^n$ is said to be q-ary for a certain integer q (possibly prime) if $q\mathbb{Z}^n \subset \mathcal{L} \subset \mathbb{Z}^n$.

Since any lattice is closed by addition, we notice that the membership of a vector $\mathbf{x}$ in $\mathcal{L}$ is determined by $\mathbf{x} \mod q$. We are going to deal with the

following two examples of q-ary lattices: given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ for some integers q, m, n, we can define

$$\mathcal{L}_q(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{A}^T\mathbf{s} \mod q \text{ for some } \mathbf{s} \in \mathbb{Z}^n\} \quad (1.5)$$

$$\mathcal{L}_q^{\perp}(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{A}\mathbf{y} = 0 \mod q\}. \quad (1.6)$$

The first lattice is generated by the rows of $\mathbf{A}$ and therefore corresponds to the code they generate. On the other hand, the second one contains all vectors that are orthogonal $\mod q$ to the rows of $\mathbf{A}$ and hence it corresponds to the code whose parity check matrix is exactly $\mathbf{A}$.

1.1.2 Computational Problems

As already stated in the introduction, many cryptosystems can be proved secure assuming the hardness of certain lattice problems in the worst case. In the following, we present the most useful among them and we briefly outline their computational complexity.

Definition 1.5 (**Shortest Vector Problem**(SVP))**.** Given an arbitrary basis $\mathbf{B}$ of a lattice $\mathcal{L} = \mathcal{L}(\mathbf{B})$, find a shortest non zero lattice vector, i.e. a $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v}\| = \lambda_1(\mathcal{L})$.

It is worth highlighting that in practice *approximation lattice problems* are those needed to get average-case to worst case reductions. These instances are parametrized by an approximation factor $\gamma \geq 1$ which usually depends on the dimension n of the lattice, i.e., $\gamma = \gamma(n)$. More precisely, in practical protocols this factor needs to be polynomial in n, i.e., $\gamma = poly(n)$.

Definition 1.6 (**Approximate Shortest Vector Problem**(SVP_γ))**.** Given an arbitrary basis $\mathbf{B}$ of an n-dimensional lattice $\mathcal{L} = \mathcal{L}(\mathbf{B})$, output a non zero lattice vector $\mathbf{v}$ such that $\|\mathbf{v}\| \leq \gamma(n) \cdot \lambda_1(\mathcal{L})$.

Definition 1.7 (**Approximate Shortest Independent Vector Problem**(SIVP_γ))**.** Given a basis $\mathbf{B}$ of an n-dimensional lattice $\mathcal{L} = \mathcal{L}(\mathbf{B})$, find a set $\mathbf{S} = \{s_i\}_{i=1}^n \subset \mathcal{L}$ of n linearly independent lattice vectors with $\|s\|_i \leq \gamma(n) \cdot \lambda_n(\mathcal{L})$ for all i.

While we previously dealt with *search* problems, the following is a *decision* one and turns out to be fundamental for LWE crytposystem security:

Definition 1.8 (**Decisional Approximate SVP**(GapSVP_γ))**.** Given an arbitrary basis $\mathbf{B}$ of an n-dimensional lattice $\mathcal{L} = \mathcal{L}(\mathbf{B})$, where either $\lambda_1(\mathcal{L}) \leq 1$ or $\lambda_1(\mathcal{L}) < \gamma(n)$, determine which is the case .

A final important problem linked to the Learnin with Errors problem is the *bounded distance decoding* problem (BDD_γ). Its aim is to find the unique lattice vector that is the closest to a given point $\mathbf{t} \in \mathbb{R}^n$ ($target$), which is promised to be "sufficiently" close to the lattice.

Definition 1.9 (**Bounded Distance Decoding Problem**(BDD_γ))**.** Given basis $\mathbf{B}$ of an n-dimensional lattice $\mathcal{L} = L(\mathbf{B})$, and a target point $\mathbf{t} \in \mathbb{R}^n$ with the guarantee that $\text{dist}(\mathbf{t}, \mathcal{L}) < d = \lambda_1(\mathcal{L})/(2\gamma(n))$, find the unique lattice vector $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{t} - \mathbf{v}\| < d$.

1.1.2.1 Algorithms

Classical Algorithms. All the problems mentioned above have been intensively studied and turn out to be intractable for approximation factor of the type $\gamma = poly(n)$. There is clearly a trade-off between the running time of algorithms and the magnitude of approximation factors: known polynomial-time algorithms (LLL [LLL82], and its descendant [Sch87] with [AKS01] as subroutine) require slightly subexponential approximation factors $\gamma = 2^{\Theta(n \log\log n/\log n)}$, while those obtaining $\gamma = poly(n)$ ([AKS01], [Kan83] and [MV10]) require at least super-exponential $2^{\Theta(n \log n)}$ time or exponential time $2^{\Theta(n)}$ and space.

Quantum Algorithms. We notice that running time above represents the state of the art also for quantum algorithms.As a matter of fact, since Shor's discovery of the quantum factoring algorithm in 1997[Sho97], any attempts to solve lattice problems by quantum algorithms have brought no significant advantages. The main reason is that the period-finding subroutine, typical of

Shor's factoring algorithm [Sch87] and related quantum algorithms, does not seem to be effective in tackling lattice problems. We can therefore formulate the following conjecture, which is at the basis of the security of any lattice based cryptographical scheme:

Conjecture 1.1.1. There is no polynomial-time classical or quantum algorithm that solve approximated lattice problems (in the worst-case) when $\gamma = poly(n)$.

1.1.3 Ideal and Cyclic Lattices

As we will notice later, while providing a high standard of security, cryptosystem based on general lattices are usually quite inefficient, mainly due to the key size they require. For this reason, protocols used in practice rely on ideal and cyclic lattices, which we now introduce.

Definition 1.10 (**Cyclic Lattices**)**.** A set $\mathcal{L} \subset \mathbb{Z}^n$ is a cyclic lattice if it is an ideal in $\mathbb{Z}[x]/(x^n - 1)$.

In practice, we can consider the **coefficient embedding**

$$\begin{aligned} \sigma : \mathbb{Z}[x]/(x^n - 1) &\longrightarrow \mathbb{Z}^n \\ \overline{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}} &\mapsto (a_0, \ldots, a_{n-1}) \end{aligned}$$

and hence we can identify $\mathcal{L}$ with $\sigma(\mathcal{L})$. In this way, since $\mathcal{L}$ is closed under multiplication by $x \mod (x^n - 1)$, we can think of a cyclic lattice as a set of n-uples in $\mathbb{Z}^n$ such that:

- for $\mathbf{v}, \mathbf{u} \in \mathcal{L}$, we have $\mathbf{v} + \mathbf{u} \in \mathcal{L}$;
- given $\mathbf{v} \in \mathcal{L}$, $-\mathbf{v} \in \mathcal{L}$;
- for $\mathbf{v} = (v_1, \ldots, v_n) \in \mathcal{L}$, any cyclic shift of its coordinates is also in $\mathcal{L}$.

Definition 1.11 (**Ideal Polynomial**)**.** A polynomial $f \in \mathbb{Z}[x]$ is an ideal polynomial if it is monic, irreducible and if for any $g, h \in \mathbb{Z}[x]$ we have $\|gh \mod f\| \leq poly(n) \|g\| \|h\|$, where $n = deg(f)$

Definition 1.12 (**f-Ideal Lattices**)**.** Let f be an ideal polynomial, then a set $\mathcal{L} \subset \mathbb{Z}^n$ is a f-ideal lattice if it is an ideal in $\mathbb{Z}[x]/(f)$.

As before, we can see an ideal of $\mathbb{Z}[x]/(f)$ as a subset o $\mathbb{Z}^n$ by the **coefficient embedding**. In addition, notice that since $x^n - 1$ is not irreducible, a cyclic lattice is not a $(x^n - 1)$-ideal lattice.

Remark 3. In the definition above, some authors require the polynomial f to be only irreducible and monic. However, since in practical application the condition on the norm is necessary, we prefer to add it in the original definition of f-ideal lattice.

Remark 4. The advantages of using these particular lattices are manifold. First of all, we can represent them by using a single n-dimensional vector, whose elements are the coefficients of the polynomial. Secondly, they have an algebraic structure that implies fast arithmetic by using FFT. Finally, as we will see later, they enable us to have smaller keys size in several cryptographical protocols.
On the other hand, there may be consistent drawbacks in terms of security. Suppose we were able to find an adequate worst-case to average-case reduction also in this setting, the safety of our protocols would be strictly linked to the chance of finding a hard instance of some lattice problem among the family of cyclic or ideal lattices. However, these lattice problems can be handled with different techniques exploiting the additional structure of ideals, thus leading to a different computational complexity. For example, it can be shown that GapSVP$_\gamma$, for $\gamma = poly(n)$, is actually easy on ideal lattices, while SVP$_\gamma$ and SIVP$_\gamma$ are equivalent problems. Anyway, they seem to be very hard in the worst case, both for classical and quantum algorithms, also in the case of cyclic and ideal lattices. Taking the above into account, while reckoning that hardness of problems on f-ideal lattices need to be further investigated, we can formulate the following conjecture:

Conjecture 1.1.2. Let $f \in \mathbb{Z}[x]$ be an ideal polynomial, then solving SVP$_\gamma$ with $\gamma = poly(n)$ in f-ideal lattices requires $2^{\Omega(n)}$ bit operations.

1.2 Gaussian Measure

Many modern cryptographical protocols make use of Gaussian-like probability distributions over lattices, known as *discrete Gaussians*. In this section we present the relevant definitions and we state some related basic results.

Definition 1.13 (**Scaled Gaussian Function**)**.** For any positive integer n and real $r > 0$, $r = 1$ when omitted, the Gaussian function $\rho_r : \mathbb{R}^n \longrightarrow \mathbb{R}+$ of parameter (or width) r is defined as

$$\rho_r = \exp(-\pi \left\|x\right\|^2 / r^2)$$

Since the total measure associated to ρ_r is $\int_{\mathbf{x}\in\mathbb{R}^n} \rho_r(\mathbf{x})\mathrm{d}\mathbf{x} = r^n$, by normalising we get the following distribution:

Definition 1.14 (**Scaled Continuous Gaussian Distribution**)**.** The (continuous) Gaussian distribution D_r of parameter(width) r over $\mathbb{R}^n$ is defined to have probability density function

$$D_r(\mathbf{x}) = \frac{\rho_r(x)}{r^n}$$

Remark 5. We notice that ρ_r is invariant under rotations of $\mathbb{R}^n$ and that $\rho_r(\mathbf{x}) = \prod_{i=1}^n \rho_r(x_i)$. Hence a sample from the Gaussian distribution D_r can be obtained by taking n independent samples from the 1-dimensional Gaussian distribution.

Definition 1.15 (**Discrete Gaussian of Parameter r**)**.** For any countable set A and any parameter(width) $r > 0$, the discrete Gaussian probability distribution $D_{A,r}$ is defined as:

$$\forall \mathbf{x} \in A,\ D_{A,r}(\mathbf{x}) \coloneqq \frac{\rho_r(\mathbf{x})}{\rho_r(A)},$$

with $\rho_r(A) = \sum_{\mathbf{x}\in A} \rho_r(\mathbf{x})$.

In this work, A will usually be taken as a lattice $\mathcal{L}$. The following two pictures, where the *z-axis* represents the probability, are examples of Discrete Gaussian over a 2-dimensional lattice.

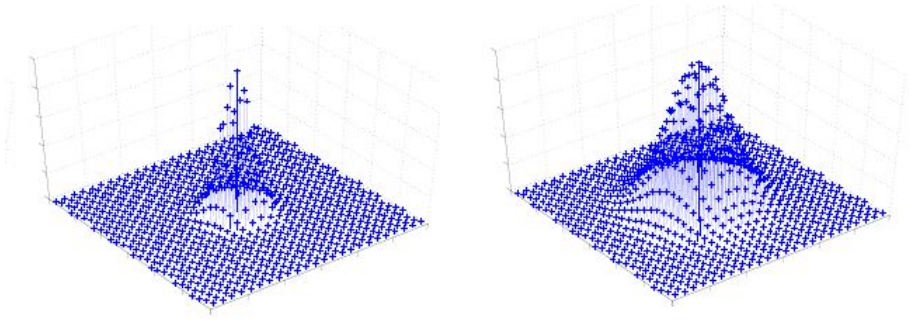

Figure 1.1: $D_{\mathcal{L},1}$ and $D_{\mathcal{L},2}$

Definition 1.16 (**Smoothing Parameter**)**.** For a lattice $\mathcal{L}$ and a positive real $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\mathcal{L})$ is defined as the smallest $\lambda > 0$ such that $\rho_{1/\lambda}(\mathcal{L}^* \setminus \mathbf{0}) \leq \epsilon$.

Definition 1.17 (**Overwhelming Probability**)**.** Given a probability space $(\Omega, \mathcal{B}, \mathcal{P})$ and $n \in \mathbb{N}$, an event $E = E(n) \in \mathcal{B}$ holds with overwhelming probability if for every $c > 0$ it holds with probability $1 - O(n^{-c})$.

Definition 1.18 (**Non-negligible Function**)**.** A real-value function $\mu : \mathbb{N} \to \mathbb{R}$ is non-negligible if $\exists\ c \in \mathbb{N}$ such that $\forall n_0,\ \exists n \geq n_0$ such that $\mu(n) \geq n^{-c}$.

Definition 1.19 (**Statistical Distance**)**.** Given two continuous random variables X_1 and X_2 over $S \subset \mathbb{R}^n$ with distribution f_1 and f_2 respectively, their statistical distance is defined as:

$$\Delta(X_1, X_2) = \frac{1}{2} \int_S |f_1(r) - f_2(r)| dr$$

Chapter 2

Early Results

In this chapter we outline some of the groundbreaking works in lattice cryptography as the Ajtai-Dwork cryptosystem [AD97] and the NTRU [HPS98]. They are public-key encryption schemes with opposite characteristics: the former admits strong provable security guarantees but is not sufficiently efficient to be used in practice, while the latter is extensively and successfully used but lacks a supporting proof of security. We will discuss them from a theoretical point of view, focusing on the idea behind them rather then on technical details. Finally, we stress that they both succeed Ajtai hash function [Ajt96a], the very first example of worst-case to average-case reduction, but this will be considered later together with the SIS problem.

2.1 Ajtai-Dwork Encryption Scheme

In their joint work from 1997 [AD97], Ajtai and Dwork described the first example of lattice based encryption scheme. On a general level, their work can be summed up as follows:

- they define an *average-case* "hidden hyperplanes problem" in $\mathbb{R}^n$ (HHP) and show that it is at least as hard as solving a variant of SVP_γ on arbitrary n-dimensional lattices;

- they describe a public-key cryptosystem whose semantic security is based on the harndess of HHP and therefore on the conjectured worst-case hardness of the above lattice problem.

Before going into further details, we underline that it is the arbitrariness of the lattices in the first point that allows us to spot worst-case reduction. We now formally define the two linked problems.

Definition 2.1 (**Hidden Hyperplanes Problems**(HPP))**.** Let $\mathbf{s} \in \mathbb{R}^n$ be a secret, random short vector. The data of the problem is a set $\{\mathbf{y}_i\}_i$, of some points $\mathbf{y}_i \in \mathbb{R}^n \ \forall\, i$, such that $\langle \mathbf{s}, \mathbf{y}_i \rangle$ is close to an integer, which means $\langle \mathbf{s}, \mathbf{y}_i \rangle \approx 0 \mod 1$. The goal of the problem is to find the secret $\mathbf{s}$.

Remark 6. We may see this problem from a geometrical point of view: for each $\mathbf{y}_i$ there exist a $j_i \in \mathbb{Z}$ such that $\mathbf{y}_i$ is close to the $(n-1)$-dimensional hyperplanes $H_{j_i} = \{\mathbf{z} \in \mathbb{R}^n : \langle \mathbf{s}, \mathbf{z} \rangle = j_i\}$ and the aim is to find the suitable $\mathbf{s}$. Furthermore, we notice that this is an *average-case* problem since $\mathbf{s}$ and the points y_i are chosen at random according to a fixed distribution.

Definition 2.2 (**Unique Approximate Shortest Vector Problem**$(uSVP_\gamma)$)**.** Let $\mathcal{L} = \mathcal{L}(\mathbf{B})$ be a lattice with a γ-unique shortest vector, i.e. $\lambda_2(\mathcal{L}) \geq \gamma \cdot \lambda_1(\mathcal{L})$, find a shortest non zero lattice vector.

Remark 7. The lattice problem above is a *worst-case* problem: we do not have a probability distribution neither on the lattice nor on its basis and therefore an algorithm is able to solve the uSVP$_\gamma$ if it can handle any lattice as an input (providing the γ-unique shortest condition).

2.1.1 Ajtai-Dwork Cryptosystem

In this paragraph, we define the actual cryposystem and examine its security and finally discuss its practical implementation.

Algorithm 1 Ajtai-Dwork cryptosystem

- **Parameters**: Integers n,m;
- **Private Key**: $\mathbf{s} \in \mathbb{R}^n$ short and random;
- **Public Key**: a set of m random points $\{\mathbf{y}_i\}_{i=1}^m$, $\mathbf{y}_i \in \mathbb{R}^n \, \forall i$, such that $\langle \mathbf{s}, \mathbf{y}_i \rangle \approx 0 \mod 1$ (i.e. $\mathbf{s}$ is a solution of HHP with data $\{\mathbf{y}_i\}_{i=1}^m$);
- **Encryption**: to encrypt 0 generate a random point $\mathbf{y}$ in $\mathbb{R}^n$; to encrypt 1 consider $\mathbf{y} = \sum_{l \in J} \mathbf{y}_l$ with $J \subset [m]$ arbitrary and finally send $\mathbf{y}$;
- **Decryption**: the receiver computes $r = \langle \mathbf{s}, \mathbf{y} \rangle$. By linearity, if $r \approx 0$ he decrypts the ciphertext as 1, otherwise as 0.

Security. Ajtai and Dwork proved the security of this cryptosystem through two independent results:

- whoever can distinguish between the encryption of 0 and 1 can also efficiently solve the HHP with the same data. This implies that breaking the semantic security of their cryptosystem is at least as hard as solving HHP (*search-to-decision* reduction);
- starting from any algorithm that solves HHP, it is possible to build one that efficiently solves uSVP_γ, in the worst case, for some $\gamma = poly(n)$.

Combining these results together, Ajtai and Dwork got a *worst-case* to *average-case* reduction, which means that breaking the cryptosystem is at least as hard as solving uSVP_γ.

Complexity and Implementation. As already mentioned, despite being a pioneering result from a theoretical point of view, this original version of the cryptosystem is quite inefficient when practically implemented. In 1998, Nguyen and Stern [NS98] developed an heuristic attack, which works efficiently for "small" parameters, to recover the private key given the classical

one. In this way, they showed that the dimension n should be of several hundreds to avoid cryptanalytic attacks, concluding that, without major improvements, Ajtai-Dwork cryptoystem is only of theoretical importance. In his subsequent work [Ajt05], Ajtai presented a more efficient version of the cryptosystem characterised by public keys and ciphertext sizes of $\widetilde{O}(n^2)$ and $\widetilde{O}(n)$ respectively. However, to date no *average-case* to *worst-case* reduction is known and although being very similar to lattice based protocol, it is built upon a problem by Dirichlet which seems not related to any known lattice problems.

2.2 NTRU Ecryption Scheme

In their 1998 joint paper [HPS98], Hoffstein, Pipher and Silverman described the public-key encryption scheme NTRU, presumably named after the expression "N-th degree truncated polynomial ring". As a matter of fact, this cryptosystem is the first protocol based on polynomial rings, in particular on f-ideal lattices. As far as performances are concerned, the NTRU is practically efficient both in terms of runtimes and keys size. These features, combined with the conjectured safety against quantum attacks, are the reasons why NTRU is widely used as an alternative to RSA and ECC. On the other hand, not much is known about the semantic security of the cryptosystem. More precisely, up to now nobody has succeeded in showing a proper *average-case* to *worst-case* reduction, thus leaving the hardness of NTRU an unsolved issue. In the following, we describe the original cryptosystem as it was presented and, later on, we briefly discuss subsequent works highlighting an evident tradeoff between performance and security.

Algorithm 2 NTRU cryptosystem

- Parameters: n power of 2, $f(X) = X^n + 1$ and q odd sufficiently large, we define $R = \mathbb{Z}[X]/(f(X))$ and $R_q = R/qR$;
- Private Key: $s, g \in R$ short polynomial, (i.e. with small coefficients) such that s is invertible $\mod q$ and $\mod 2$;
- Public Key: $h = 2g \cdot s^{-1} \in R_q$ with $g \in R$ short polynomial;
- Encryption: choose a short $e \in R$ such that $e \mod 2$ encodes the desired bit, choose $r \in R_q$ random and compute the ciphertex $c = h \cdot r + e \in R_q$;
- Decryption: multiply the ciphertext and the secret key to get $c \cdot s = 2g \cdot r + e \cdot s \in R_q$, lift it in R as $2g \cdot r + e \cdot s$ (possible if g, r, e, s are short enough compared to q) and reduce it $\mod 2$ obtaining $e \cdot s \mod 2$ and therefore the initial bit.

Variants and Implementation. Since the first version of the cryptosystem, many different variants have been developed also enabling the digital signature scheme NTRUSign [HPS01], as well as overall improvement in performances. Nowadays, the NTRUEncypt is a standard public key cryptosystem (IEEE Std. 1363.1) successfully commercialised or available under a free open source license. In the version we just presented, we may notice that both private and secret keys require $O(n \log q)$ bits to be encoded. NTRU's parameters and performances are briefly summed up in the following table:

n	q	key size	estimated security
257	2^{10}	2570 bits	80 bits
449	2^8	3592 bits	80 bits
797	2^{10}	7970 bits	256 bits
14303	2^8	114424 bits	256 bits

However, as already remarked, no version so far developed of NTRU is provided either with an average-case to worst-case reduction or with a more general security proof. With this goal in mind, in 2011 Stehle and Steinfeld proposed a variant of the NTRU cryptsystem which has been proved secure assuming the hardness of a certain lattice problem([SS11]). Unfortunately, to get a reasonable standard of safety, the pratical instantiation is significantly less efficient than the original scheme and this depicts the general trend between security and performances, which unfortunately seems to linger on lattice based cryptography.

Chapter 3

Modern Results

In modern lattice cryptography almost all protocols are based on two average-case computational problems: the Short Integer Solution problem (SIS) and the Learning with Errors problem (LWE). In this chapter, we introduce them highlighting their main features and analogies. Furthermore, we discuss their hardness and some basic cryptosystems relying on them.

3.1 SIS and Related Protocols

The Short Integer Solution was defined by Ajtai in [Ajt96a] and used to develop a conjectured one-way and collision resistant hash function known as Ajtai function. Being this work the first example of worst-case to average-case reduction involving lattice problems, its importance goes well beyond the hash function itself, which actually turns out to be quite inefficient. Many different cryptographical tools, like identification scheme[Lyu08, KTX08] and digital signature schemes[CHK09, GPV08, Boy10, MP12], have been based on the SIS. However, up to now no public-key encryption scheme has been developed yet. In the following section, after formally defining the SIS problem and discussing some of its properties, we introduce the original Ajtai function and some later and more performant versions.

3.1.1 Short Integer Solution Problem(SIS)

At the highest level, given a set of uniformly random elements of an additive group, the SIS problem consists in finding a sufficiently "short" nontrivial integer combination of them summing to zero. More specifically, SIS is parametrized by positive integers n, q, m, with $q > 2$ prime, defining $\mathbb{Z}_q^n$ and the number of group elements, and a positive real β which accounts for the shortness of the solution. We will further discuss these parameters and their practical magnitude after the formal definition of SIS.

Definition 3.1 (**Short Integer Solutions (SIS$_{n,q,\beta,m}$)**)**.** Given m uniformly random vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$, grouped as the columns of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find a nonzero integer vector $\mathbf{z} \in \mathbb{Z}^m$, $\|z\| \leq \beta < q$, such that

$$f_{\mathbf{A}}(\mathbf{z}) \coloneqq \mathbf{A}\mathbf{z} = \sum_{i=1}^{m} \mathbf{a}_i \cdot z_i = 0 \in \mathbb{Z}_q^n \tag{3.1}$$

Remark 8. We now make some general notes and we briefly focus on the choice of parameters:

- n is the main harder parameter, usually in the hundreds, while q and β are both polynomials in n;
- the condition $\beta < q$ is crucial to exclude trivial but otherwise consistent solutions $\mathbf{c}_i = (0, \dots, q, \dots)$, with q in the i-th position and $i \in [m]$;
- without an upper bound on $\|z\|$, the problem can be solved in polynomial time by applying Gaussian reduction;
- since any solution for a matrix $\mathbf{A}$ can be modified into a solution of the problem with any matrix of the kind $[\mathbf{A} \,|\mathbf{A}']$, SIS can only become easier as m increases.

.

We now try to find conditions on the parameters that guarantee the existance of a solution for SIS. Given the last remark, we would like to keep m as small as possible.

Proposition 3.1.1. *Let $\overline{m} = \lceil n \log q \rceil$, $m \geq \overline{m}$ and $\beta \geq \sqrt{\overline{m}}$, then the SIS problem admits at least one solution $\boldsymbol{z} \in \mathbb{Z}^m$.*

Proof. First of all, we may assume $m = \overline{m} = \lceil n \log q \rceil$ by the last remark. We have therefore more than q^n vectors $\mathbf{x} \in \{0,1\}^m$ as $q^n < 2^m$, thus there must be two distinct $\mathbf{x}, \mathbf{y} \in \{0,1\}^m$ such that $\mathbf{Ax} = \mathbf{Ay} \in \mathbb{Z}_q^n$. We can now consider $\mathbf{z} = \mathbf{x} - \mathbf{y} \in \{0, \pm 1\}$ which is a solution whose norm is at most β and this ends the proof. □

SIS as a lattice problem. As we already stated, SIS can be interpreted as an *average*-case problem over a family of q-ary lattices. We recall from **Definition 1.6** that

$$\mathcal{L}_q^{\perp}(\mathbf{A}) \quad = \quad \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{Ay} = 0 \mod q\}$$

and we highlight that any nonzero short vector in this kind of lattices is equivalent to an integer linear combination of columns of $\mathbf{A}$ that sums to 0; i.e. the SIS problem asks to find sufficiently short nonzero vectors in $\mathcal{L}_q^{\perp}(\mathbf{A})$, with $\mathbf{A}$ chosen at random. Taking this into account, the conjectured hardness of SIS will derive from showing that solving this average-case lattice problem would imply being able to solve some other lattice problem in its worst case.

Remark 9. We can also define the inhomogeneus version of the SIS, which asks to find short integer solutions to $\mathbf{Ax} = \mathbf{u}$ with $\mathbf{A}$ and $\mathbf{u}$ uniformly random and independent. If we ignore the norm bound, using the lattice formulation above we get that the set of solutions of this problem is the lattice coset $\mathcal{L}_u^{\perp}(\mathbf{A}) \coloneqq \mathbf{c} + \mathcal{L}_q^{\perp}(\mathbf{A})$ where $\mathbf{c}$ is an arbitrary solution.

Hardness. Following Ajtai's worst-case to average-case reduction many different improvements on estimating SIS hardness have been done. This series of results is summed up in this theorem:

Theorem 3.1.2. *For any $m = poly(n)$, any $\beta > 0$, and any sufficiently large $q \geq \beta \cdot poly(n)$, solving $SIS_{n,q,\beta,m}$ is at least as hard as solving the decisional approximate shortest vector problem $GapSVP_\gamma$ and the approximate shortest independent vectors problem $SIVP_\gamma$ on arbitrary n-dimensional lattices, for some $\gamma = \beta \cdot poly(n)$.*

Remark 10. First of all we may notice that the main hardness parameter is n, as m plays no major role in the statement. In addition, it is worth highlighting that the reduction is entirely classical and this is a substantial difference from LWE where, as we will see, it involves quantum computing.

Remark 11. Many of the different proofs of this reduction [CN97, Mic04, MR07] consist in finding iteratively set of linearly independent vectors of shorter and shorter length using an oracle for SIS. On the other hand, Micciancio and Peikert[MP13] introduce the Gaussian lattice sampling (i.e. sampling lattice vectors according to a Gaussian distribution of progressively small width) as an intermediate problem and succeded in sharpening the bound on q to $\beta \cdot n^\epsilon$ for any $\epsilon > 0$.

3.1.2 Lattice-based hash function

We briefly recall that an hash function is a function $h : \mathcal{D} \longrightarrow \mathcal{C}$ where $|\mathcal{D}| \gg |\mathcal{C}|$. Furthermore, h is said to be *one-way* when it is hard to invert and *collision resistant* when finding distinct $x, y \in \mathcal{D}$ such that $h(x) = h(y)$ is hard from a computational point of view. Nowadays, in order to be sufficiently performant, hash functions rely on ad-hoc design principles similar to those typical of block ciphers. However, the recent development of several attacks (MD5, SHA-1, Nostradamus and Herdin) has stimulated research of theoretical constructions whose security can be linked to some underlying mathematical problem. As for encryption schemes, lattice problems stand out among all the possibilities for their conjectured hardness with respect to quantum attacks. In the following, we formally define Ajtai's function and discuss its main features, then we focus on subsequent improved versions

which have led to the SWIFFT [LMP12], the very first highly efficient lattice based hash function.

3.1.2.1 Ajtai's function

We recall that the $\text{SIS}_{n,q,\beta,m}$ problem consists in finding short integer nonzero solutions $\mathbf{z} \in \mathbb{Z}^m$ of (3.1):

$$f_{\mathbf{A}}(\mathbf{z}) = \mathbf{A}\mathbf{z} = \sum_{i=1}^{m} \mathbf{a}_i \cdot z_i = 0 \in \mathbb{Z}_q^n$$

where short means $\|z\| \leq \beta < q$ and $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ is a random matrix . Let us now consider the following family of functions:

Algorithm 3 Ajtai Hash function

- **Parameters**: Integers q, n, m with $q > 2$ and prime;
- **Key**: $\mathbf{A}$ uniformly random in $\mathbb{Z}_q^{n \times m}$;
- **Hash Function**:

$$\begin{aligned} f_{\mathbf{A}}^* \colon \{0,1\}^m &\to \mathbb{Z}_q^n \\ \mathbf{x} &\mapsto \mathbf{A}\mathbf{x} \mod q \end{aligned} \tag{3.2}$$

We can observe that, assuming the hardness of the corresponding SIS problem, 3.2 is collision resistant: having a collision $\mathbf{x}, \mathbf{y} \in \{0,1\}^m$ for $f_{\mathbf{A}}^*$ would mean having a short solution $\mathbf{z} = \mathbf{x} - \mathbf{y}$ for (3.1). To sum up, using the worst-case to average-case reduction of **Theorem 3.1.2**, we get that finding collisions for the family of functions $F_{\mathbf{A}} = \{f_{\mathbf{A}}^* \to \{0,1\}^m \to \mathbb{Z}_q^n, \mathbf{A} \in \mathbb{Z}_q^{n \times m}\}$ is at least as hard as solving GapSVP_γ and SIVP_γ. Furthermore, Ajtai proved[Ajt96a] that these functions are difficult to invert on average, thus obtaining a family of one-way and collision resistant hash functions.

Remark 12. We note that from **Proposition 3.1.1** we have that $m > n \log q$ so the function defined by Ajtai indeed compresses the input. The paramenter m should be therefore chosen bearing in mind the tradeoff between the level of compression and the assumption of collision-freedom (as m grows, SIS become easier).

Efficiency. Despite being very simple to implement, as it requires only a matrix-vector product and a reduction modulo $q = poly(n)$, Ajtai function turns out to be not useful for practical applications. The main reason of its inefficiency is the key size $\tilde{O}(mn)$, at least quadratic in n, which implies a great cost in terms of space and time to guarantee a high standard of security. In their work [MR09], Micciancio and Regev showed that in order to get 100 bits of security, the key size and the arithmetic operations need to be at least of 500,000 bits and 50,000 respectively, way too much for a simple cryptographic primitive like hash functions.

3.1.2.2 Hash functions on cyclic lattices

The efficiency of lattice-based hash functions above can be dramatically improved by using in **Algorithm 3** matrices with particular structure in place of general ones. We can for example consider, for $n|m$, the block-matrix $\mathbf{A} = [\mathbf{A}^{(1)}| \dots |\mathbf{A}^{(m/n)}]$, where each block $\mathbf{A}^{(i)} \in \mathbb{Z}_q^{n \times n}$ is a circulant matrix:

$$\mathbf{A}^{(i)} = \begin{bmatrix} a_1^{(i)} & a_n^{(i)} & \dots & a_3^{(i)} & a_2^{(i)} \\ a_2^{(i)} & a_1^{(i)} & \dots & a_4^{(i)} & a_3^{(i)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1}^{(i)} & a_{n-2}^{(i)} & \dots & a_1^{(i)} & a_n^{(i)} \\ a_n^{(i)} & a_{n-1}^{(i)} & \dots & a_2^{(i)} & a_1^{(i)} \end{bmatrix} \tag{3.3}$$

which means that all the columns are cyclic rotations of the first one $a^{(i)} = (a_1^{(i)}, \dots, a_n^{(i)})$. In the following, to highlight its particular structure, we denote $\mathbf{A}$ with $\mathbf{A}_{circ}$, even if $\mathbf{A}$ is not a cirulant matrix itself. To sum up, we are considering the family of hash function $F_{\mathbf{A}_{circ}}$ given in the following

algorithm.

Algorithm 4 Hash function based on cyclic lattices

- **Parameters**: Integers q, n, m, with $n|m$, $q > 2$ and prime;
- **Key**: m/n vectors $\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(m/n)} \in \mathbb{Z}_q^n$ independent and uniformly random where each $\mathbf{a}^{(i)}$ determines the circulant matrix $\mathbf{A}^{(i)}$;
- **Hash Function**:

$$\begin{aligned} f_{\mathbf{A}}^{circ}\colon \{0,1\}^m &\to \mathbb{Z}_q^n \\ \mathbf{x} &\mapsto [\mathbf{A}^{(1)}|\ldots|\mathbf{A}^{(m/n)}]\mathbf{x} \mod q \end{aligned} \tag{3.4}$$

Efficiency. Imposing such a structure on the matrices increases the efficiency for the following two reasons:

- the public key consists now in only m elements in $\mathbb{Z}_q$ rather than nm since each $\mathbf{A}^{(i)}$ is determined by its first column;
- the matrix-vector product $\mathbf{A}_{circ}\mathbf{x} \mod q$ can be performed asymptotically in $\widetilde{O}(m)$ arithmetic operations over $\mathbb{Z}_q$ rather then $O(mn)$ since Fast Fourier Transform computes multiplication by a circulant matrix in $\widetilde{O}(m)$ time.

One wayness and collision resistance. Since our choice of matrix is no longer random over $\mathbb{Z}_q^{n\times m}$, we are not actually considering an instance of the SIS, being it an average-case problem over the family of q-ary lattices $\{\mathcal{L}_q^{\perp}(\mathbf{A}), \mathbf{A} \in \mathbb{Z}_q^{n\times m} \text{ random}\}$. As a matter of fact, we are taking into account a strictly smaller set of lattices and hence, we can no longer rely on **Theorem 3.1.2** to prove that functions in $F_{\mathbf{A}_{circ}}$ are one-way and collision resistant. In his paper [Mic07], Micciancio was able to show that this efficient version of Ajtai function is hard to invert on the average as long as solving SVP_γ

is hard in the worst case over cyclic lattices (i.e. ideals of $\mathbb{Z}[X]/(X^n - 1)$, see **Definition 1.10**). Up to now, no (quantum) algorithms exploiting this cyclic structure and capable of solving SVP_γ is known and it is conjectured that no significant speed up can ever be obtained, giving confidence in the one-wayness of Micciancio's model. Furthermore, we notice that we lost the equivalence with the GapSVP_γ, but this is not a surprise as we already mentioned in the first chapter that this specific problem is easily solvable in structured lattices.
On the other hand, Lyubachevsky and Micciancio [LM06] and Peikert and Rosen [PR06] proved, using zero divisors of $\mathbb{Z}[X]/(X^n - 1)$, that in general $f \in F_{\mathbf{A}_{circ}}$ do not enjoy the property of collision resistance, i.e. finding short vectors in $\mathcal{L}_q(A_{circ})$ is not difficult in the worst case. Although one-way functions are not strong enough to be used in practical applications, these results have encouraged further research aimed at finding a proper family of lattices capable of ensuring both security and efficiency.

3.1.3 Hash functions on ideal lattices

As well as being able to prove that (3.4) is not collision-resistant, Lyubachevsky and Micciancio [LM06] succeded in finding a related function with this property. They adapted **Algorithm 3**, using this time block matrices $\mathbf{A} = [\mathbf{A}^{(1)}|\cdots|\mathbf{A}^{(m/n)}]$ where each block is defined as

$$\mathbf{A}^{(i)} = \mathbf{F}^* \mathbf{a}^{(i)} \coloneqq [\mathbf{a}^{(i)}, \mathbf{F}\mathbf{a}^{(i)}, \ldots, \mathbf{F}^{n-1}\mathbf{a}^{(i)}]$$

with

$$\mathbf{F} \coloneqq \left[\begin{array}{ccc|c} & \mathbf{0}^T & & f_1 \\ \hline \ddots & & & f_2 \\ & \mathbf{I} & & \vdots \\ & & \ddots & f_n \end{array}\right] \quad \text{and} \quad \mathbf{f} \coloneqq (f_1, \ldots, f_n) \in \mathbb{Z}^n$$

Furthermore, in order to be in the setting of f-ideal lattices, they impose the following conditions on $\mathbf{f}$:

- $\hat{f}(x) = x^n + f_n x^{n-1} + \cdots + f_1 \in \mathbb{Z}[x]$ is irreducible;
- for any $g, h \in \mathbb{Z}[x]$ we have $\|gh \mod f\| \leq poly(n)\,\|g\|\,\|h\|$.

Eventually, they get the following hash function:

Algorithm 5 Hash function based on f-ideal lattices

- **Parameters**: Integers q, n, m, with $n|m$,with $q > 2$ and prime, $\mathbf{f} \in \mathbb{Z}^n$ with the conditions above;
- **Key**: m/n vectors $\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(m/n)} \in \mathbb{Z}_q^n$ independent and uniformly random;
- **Hash Function**:

$$\begin{aligned} f_{\mathbf{A}}^{id} \colon \{0,1\}^m &\to \mathbb{Z}_q^n \\ \mathbf{x} &\mapsto [\mathbf{F}^*\mathbf{a}^{(1)}| \ldots |\mathbf{F}^*\mathbf{a}^{(n)}]\mathbf{x} \mod q \end{aligned} \tag{3.5}$$

Remark 13. It can be shown that taking $\mathbf{f} = (-1, 0, \ldots, 0)$ results in having the same circulant blocks of **Algorithm 4**. However, this choice is not permitted in the setting above as the correspondent $\hat{f} = x^n - 1$ is not irreducible. Finally, we highlight that the previous remarks on efficiency, regarding keys size and number of arithmetic operations needed to evaluate the product matrix-vector, still holds in this case.

One-wayness and collision resistance. Micciancio and Lyubashevsky were able to prove that besides being one-way, functions (3.5) are collision-resistant, equivalently finding short vectors in $\mathcal{L}_q^{\perp}([\mathbf{F}^*\mathbf{a}^{(1)}| \ldots |\mathbf{F}^*\mathbf{a}^{(n)}])$ is difficult, as long as solving SVP_γ on $\hat{f}$-ideal lattices (ideals of $\mathbb{Z}[x]/(\hat{f}(x))$ see **Definition 1.11**) is hard in the worst case. As already asserted in *Conjecture 1.1.2*, despite lacking a formal proof, we may assume that the above holds, even for quantum algorithms, making $f_{\mathbf{A}}^{id}$ a collision resistant and one-way

hash function.

SWIFFT hash function. We now briefly sketch the main features of the SWIFFT, which is the most efficient concrete instantiation of collision resistant function based on SIS. Introduced in [LMP12], basically it is a highly optimized variant of **Algorithm 5**, which additionally exploits a wise choice of modulus q and a pre/post processing operation applied to the key and the output of the hash function. More precisely, $\mathbf{f}$ is chosen to be $\mathbf{f} = (1, \ldots, 0)$, and we notice that the corresponding polynomial $\hat{f} = X^n + 1$ verifies the conditions required in the previous model. As a result, $\mathbf{F}$ is a cyclic rotation of the coordinates with the sign of those wrapped around changed and each block $A^{(i)}$ is a circulant matrix, with the element above the diagonal with opposite sign. Lyubashevsky *et al.* proposed the following parameters which guarantees a high level of both security and efficiency:

n	m	q	key size	input size	output size	security
64	1024	257	8192 bits	1024 bits	513 bits	100 bits

3.2 LWE and Related Protocols

In his seminal work from 2005 [Reg05] , Regev introduced the average-case problem known as Learning with Errors Problem. Since then, not only it has appeared as the most apt lattice problem to support an encryption scheme but it has also shown its versatility enabling chosen ciphertext-secure cryptosystem [PW08], identity based encryption scheme [GPV08, Pei09b, CHK09] and fully homomorphic encryption [BV12, BGV14, GSW13] . We now describe LWE in details and outline its main properties, then we discuss its hardness and finally we introduce a simple cryptosystem based on it. We remark that in this section we are going to deal with LWE for general lattices, while the ring version (i.e. over f-ideal lattices) will be the topic of next chapter.

3.2.1 Learning With Errors Problem(LWE)

LWE is parametrized by three positive integers n, q and m, defining $\mathbb{Z}_q^n$ and the number of samples available, and by an error distribution χ over $\mathbb{Z}$. In practice, n,q and m play the same role they do in SIS, while χ can be thought as a discrete Gaussian of width αq for some $\alpha < 1$, i.e. $\chi = D_{\mathbb{Z},\alpha q}$. We now define the LWE distribution and the two versions (*search* and *decision*) of the LWE problem.

Definition 3.2 (**LWE Distribution**)**.** For a vector $\mathbf{s} \in \mathbb{Z}_q^n$, called secret, the LWE distribution $A_{\mathbf{s},\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is sampled by choosing $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, choosing $e \leftarrow \chi$, and outputting $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e \mod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Definition 3.3 (**Search-LWE**$_{n,q,\chi,m}$)**.** Given m independent samples $\{(\mathbf{a}_i, b_i)\}_{i=1}^m \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ drawn from $A_{\mathbf{s},\chi}$, with $\mathbf{s}$ chosen uniformly at random, find $\mathbf{s}$.

Basically, we are trying to find $\mathbf{s} \in \mathbb{Z}_q^n$ solution of the system of linear "equations with errors":

$$\begin{aligned} \langle \mathbf{s}, \mathbf{a}_1 \rangle &= b_1 - e_1 \mod q \\ \langle \mathbf{s}, \mathbf{a}_2 \rangle &= b_2 - e_2 \mod q \\ &\vdots \\ \langle \mathbf{s}, \mathbf{a}_m \rangle &= b_m - e_m \mod q \end{aligned}$$

with each $\mathbf{a}_i$ uniformly random and each e_i output of χ. We remark that the error vector $\mathbf{e} = (e_1, \ldots, e_n)$ is not known but the discrete probability distribution is a datum of the problem.

Definition 3.4 (**Decision-LWE**$_{n,q,\chi,m}$)**.** Given an error distribution χ over $\mathbb{Z}$ and m independent samples $\{(\mathbf{a}_i, b_i)\}_{i=1}^m \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where every sample is distribuited according to either: (1) $A_{\mathbf{s},\chi}$ for a fixed and uniformly random $\mathbf{s} \in \mathbb{Z}_q^n$, or (2) the uniform distribution, distinguish which is the case.

Remark 14. As for SIS, we now make some general notes:

- without the errors coming from the distribution χ both the search and decision version of the problem can be efficiently solved by applying Gaussian elimination;
- we can represent the LWE problem in a more compact way by using matrices: the random set $\{(\mathbf{a}_i)\}_{i=1}^{i=m}$ can be viewed as columns of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ while the respective $(b_i = \langle \mathbf{s}, \mathbf{a}_i \rangle + e_i \mod q)$ can make up the vector $\mathbf{b} \in \mathbb{Z}_q^m$. In addition, having $\mathbf{e} \leftarrow \chi^m$ we get:

$$\mathbf{b}^T = \mathbf{s}^T \mathbf{A} + \mathbf{e}^T \mod q. \tag{3.6}$$

LWE as a lattice problem. As well as SIS, also Search-LWE can be equivalently presented as an average case bounded-distance decoding problem (BDD_γ) over the family of q-ary lattices (1.5)

$$\mathcal{L}_q(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{A}^T \mathbf{s} \mod q \text{ for some } \mathbf{s} \in \mathbb{Z}^n\}.$$

Using the matrix notation of (3.6), the vector $\mathbf{b}$ is relatively close to a unique vector in $\mathcal{L}_q(\mathbf{A})$ and we can notice that LWE problem consists in finding this "target".

LWE and learning from parity with error. LWE can be seen as a more complex version of the well-known and studied problem "learning from parity with error" which we now define.

Definition 3.5 (**Learning from Parity with Error**)**.** Given $\epsilon > 0$ and a set of equations:

$$\begin{aligned} \langle \mathbf{s}, \mathbf{a}_1 \rangle &\approx_\epsilon b_1 \mod 2 \\ \langle \mathbf{s}, \mathbf{a}_2 \rangle &\approx_\epsilon b_2 \mod 2 \\ &\vdots \end{aligned}$$

with $\mathbf{a}_i$ uniform and independent over $\mathbb{Z}_2^n$ and each b_i chosen to be equal to $\langle \mathbf{s}, \mathbf{a}_i \rangle$ with probability 1-ϵ, find the secret $\mathbf{s} \in \mathbb{Z}_2^n$.

As a matter of fact, LWE is a genaralization of the problem above on higher moduli as the learning from parity with error is a specific case of LWE with $q = 2, \chi(0) = 1 - \epsilon$ and $\chi(1) = \epsilon$.

Hardness. Since its introduction, LWE has seemed computationally hard for its relations with BDD_γ and the learning from parity with error problem, which are both thought to be not solvable in polynomial time. In addition to this feeling, Regev proved the following worst-case to average-case reduction involving the decision version of LWE :

Theorem 3.2.1 ([Reg05])**.** *For any $m = poly(n)$, any $q \leq 2^{poly(n)}$, and any discrete Gaussian error distribution χ of parameter $\alpha q \geq 2\sqrt{n}$, with $0 < \alpha < 1$, solving the Decision-LWE$_{n,q,\chi,m}$ is at least as hard as quantumly solving GapSVP$_\gamma$ and SIVP$_\gamma$ on arbitrary $n-$dimensional lattices, for some $\gamma = \tilde{O}(n/\alpha)$.*

First of all, we may notice that the reduction involves quantum computing. Despite this seems to bring no significant advantages in dealing with GapSVP_γ and SIVP_γ (see Paragraph 1.1.2.1), it would be important to have a totally classical reduction to enhance confidence in LWE hardness. Furthermore, the proof is made up by two independent parts:

- a quantum reduction from LWE-search to GapSVP_γ and SIVP_γ, i.e. an oracle for the search version of LWE can be efficiently transformed into a quantum algorithm able to solve the above lattice problems;
- a classical search to decision reduction, i.e. Decision-LWE is at least as hard as Search-LWE.

By merging these results we get the worst-case to average-case reduction for Decision-LWE.

Remark 15. In his work from 2009 [Reg05], Peikert was able to make the above reduction entirely classical, provided these two caveats:

- the classical reduction only involves GapSVP_γ, while the quantum works also for SIVP_γ;
- the modulus q is required to be exponentially large, more precisely $q \geq 2^{n/2}$, while in Regev's theorem it suffices $q \geq 2\sqrt{n}/\alpha$ with $0 < \alpha < 1$;

The increased magnitude of q implies more bits to encode the samples and the secret of LWE, which translates in larger key sizes an less efficincy for all cryptographic protocols based on this problem. On the other other hand, the method used by Peikert to get his reduction has turned out to be very useful for a different goal: exploiting the underlying idea, Lyubashevski and Micciancio[LM09] successfully proved that, for $\gamma = poly(n)$, GapSVP_γ, uSVP_γ and BDD_γ are all equivalent problems.

3.2.2 LWE Encryption Scheme

We now present the first public key cryptosystem whose semantic security is based on LWE, presented by Regev in [Reg05]. In the following, we discuss its main advantages with respect to previously introduced lattice based cryptosystems and finally we outline the choice of paramters that can guarantee both security and correctness to the scheme.

Algorithm 6 LWE public key cryptosystem

- **Parameters**: n, q, m positive integers, $\alpha \in \mathbb{R}$ such that $0 < \alpha < 1$ and $\chi = D_{\mathbf{z},\alpha q}$ discrete distribution over $\mathbb{Z}$;
- **Private Key**: $\mathbf{s} \in \mathbb{Z}_q^n$ uniformly at random;
- **Public Key**: select m vectors $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$ indipentently according to the uniform distribution. In addition, draw $e_1, \ldots, e_m \in \mathbb{Z}$ from χ and get the public key $\{(\mathbf{a}_i, b_i)\}_{i=1}^m$, with $b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \mod q$;
- **Encryption**: let $\mu \in \{0, 1\}$ be the bit to encode, choose a random set $S \subset [m]$, then to encrypt μ one sends $(\mathbf{a}, b) = (\sum_{i \in S} \mathbf{a}_i, \sum_{i \in S} b_i + \mu \lfloor \frac{q}{2} \rfloor)$

- **Decryption**: if $b - \langle \mathbf{a}, \mathbf{s} \rangle$ is close to 0 than to $\lfloor \frac{q}{2} \rfloor \mod q$ output 0, otherwise decripts as 1.

Remark 16. By analizing encryption and decryption of **Algorithm 5**, we may notice that the choice of parameters is responsible for the correctness of the crytpographic protocols. For example, if $\mu = 0$ we need χ and q to be such that

$$b - \langle \mathbf{a}, \mathbf{s} \rangle = \sum_{i \in S} e_i < q/4, \tag{3.7}$$

otherwise the bit would be decrypted as 1. We notice that, for instance, we can get (3.7) by requiring q significantly larger than the error distribution χ and m. In order to make this cryptosystem secure (i.e. a passive eavesdropper who can distinguish between 0 and 1 can solve Decision-LWE$_{n,q,\chi,m}$) and correct at the same time, Regev proposed and showed[Reg05] that the following the setting of parameters can guarantee both: q prime between n^2 and $2n^2$ with n in the order of hundreds, $m = (1+\epsilon)(n+1)\log q$ for an arbitrary $\epsilon > 0$ and finally $\chi = D_{\mathbb{Z},\alpha(n)}$ for $\alpha(n) = 1/(\sqrt{n}\log^2 n)$.

Remark 17. We notice that, following the choice of parameters above, the secret and public keys sizes are respectively $\tilde{O}(n)$ and $\tilde{O}(mn \log q) = \tilde{O}(n^2)$. Furthermore, it is possible to reduce the public key size to $\tilde{O}(m \log q) = \tilde{O}(n)$ by exploiting this idea by Ajtai[Ajt96b]: the set of vectors $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ can be shared by all users and distributed as part of the encryption and decryption software thus leading to the public key $b_1, \ldots, b_m$. It can be proved that this change does not affect the security of the cryptosytem, which is actually thought to be greater than Ajtai-Dwork cryptosystem's, as uSVP$_\gamma$ (the mathematical problem underlying) is more structured than SIVP$_\gamma$ and GapSVP$_\gamma$.

Chapter 4

Ring-Learning With Errors Problem

The improved efficiency obtained by considering algebraic structured lattices in cryptosystems[HPS98] and hash functions[LMP12] suggested further research on problems regarding these lattices that could be used as security-guarantee for cryptographic protocols. With this goal in mind, Lyubashevsky, Peikert and Regev introduced the ring-learning with errors problem[LPR12], an analogue problem of the LWE in the ring setting, whose hardness can be linked to some worst-case problem over ideal lattices. In this chapter, we are going to introduce this problem, focusing on the worst-case to average-case reduction developed in [LPR12, LPR13] .

4.1 Background

We now introduce some concepts we will need to define and discuss the R-LWE. In the following, we fix K as a number field of degree n and we let $R = \mathcal{O}_K$ to be its ring of algebraic integers.

4.1.1 Space H, Distributions and Lattices

Space H. Since we are working with number fields and ideal lattices it is convenient to introduce the space $H \subset \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$, with $s_1 + 2s_2 = n$, for some positive integers s_1, s_2 and n whose roles will be specifed in the next section. We define:

$$H = \{(x_1, \ldots, x_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} : x_{s_1+s_2+j} = \overline{x_{s_1+j}} \quad \forall j \in [s_2]\} \subset \mathbb{C}^n.$$

It can be proved that H, with the inner product induced by $\mathbb{C}^n$, is isomorphic to $\mathbb{R}^n$ as an inner product space, by defining the following orthonormal basis $\{\mathbf{h}_i\}_{i\in[n]}$:

Definition 4.1. For $j \in [n]$ let $\mathbf{e}_j$ be the vector with 1 in its j-th coordinate and 0 elsewhere. Then we define $\mathbf{h}_j = \mathbf{e}_j$ for $j \in [s_1]$, while for $s_1 < j \leq s_1+s_2$ we define $\mathbf{h}_j = \frac{1}{\sqrt{2}}(\mathbf{e}_j + \mathbf{e}_{j+s_2})$ and $\mathbf{h}_{j+s_2} = \frac{\sqrt{-1}}{\sqrt{2}}(\mathbf{e}_j - \mathbf{e}_{j+s_2})$.

We can also equip H with the l_p norm induced from $\mathbb{C}^n$ and defined in the following way. For each element $\sum_{i=1}^n a_i\mathbf{h}_i \in H$, with $a_i \in \mathbb{R}\ \forall i$, its p-norm for $p \in [1, \infty]$ is:

$$\left\| \sum_{i=1}^{n} a_i \mathbf{h}_i \right\|_p = \left(\sum_{i=1}^{s_1} |a_i|^p + 2 \sum_{i=s_1+1}^{s_1+s_2} \left(\frac{a_i^2 + a_{i+s_2}^2}{2} \right)^{p/2} \right)^{1/p}$$

Lattices and Gaussian Measures. From now on, we will adress to lattices as discrete additive subgroup of H, i.e.

$$\mathcal{L} = \mathcal{L}(\mathbf{B}) = \{\sum_{i\in[n]} z_i\mathbf{b}_i \text{ such that } \mathbf{z} \in \mathbb{Z}^n\}$$

with $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \in H$ set of n linear independent vectors.
As we previously did in the case of $\mathbb{R}^n$, for $r > 0$ we can define the Scaled Gaussian Function $\rho_r : H \to (0, 1]$ as $\rho_r = \exp(-\pi \|x\|^2 / r^2)$. In addition, we indicate with D_r the Continuous Gaussian Distribution of width r over H, which is the probability distribution with density $s^{-n} \cdot \rho_r(\mathbf{x})$. Furthermore,

for a lattice $\mathcal{L} \subset H$ we define the Discrete Gaussian of Parameter r over $\mathcal{L}$ as:

$$D_{\mathcal{L},r} = \frac{\rho_r(\mathbf{x})}{\rho_r(\mathcal{L})} \quad \forall \mathbf{x} \in \mathcal{L}.$$

We are also going to use the following Gaussian distribution over H, which is defined by n different parameters rather than one unique.

Definition 4.2 (**Elliptical Gaussian Distribution**)**.** Given $\mathbf{r} = (r_1, \ldots, r_n) \in (\mathbb{R}^+)^n$ such that $r_{j+s_1+s_2} = r_{j+s_1}$ for each $j \in [s_2]$, a sample from $D_{\mathbf{r}}$ is given by $\sum_{i\in[n]} x_i \mathbf{h}_i$ where each x_i is chosen independently from the one-dimensional Gaussian distribution D_{r_i} over $\mathbb{R}$.

4.1.2 Ideal Lattices and Canonical Embedding

As already stated, the R-LWE is an average-case problem with a worst-case reduction to problems on structured lattices. However, the setting is slightly different from those of f-Ideal Lattices, since the choice of the embedding $\sigma : K \to \mathbb{C}^n$ of the number field plays a significant role in the definition. Before formally defining ideal lattices we recall that given K a number field of degree n and $R = \mathcal{O}_K$ its ring of integers, an integral ideal $\mathcal{I} \in R$ is an additive subgroup closed under multiplication by elements of R. Furthermore, such an ideal is finitely generated over R and is a free $\mathbb{Z}$-module of rank n, i.e. it is generated by $\mathbb{Z}$-linear combinations of a basis $\{u_1, \ldots, u_n\} \subset R$. Finally, we remark that the norm of an ideal $\mathcal{I}$ is its index as an additive subgroup of $\mathcal{O}_K$, which means $\mathcal{N}(\mathcal{I}) = |\mathcal{O}_K/\mathcal{I}|$, and that any $\mathcal{I} \subset \mathcal{O}_K$ can be factorized in a unique way as a product of powers of prime ideals.

Definition 4.3 (**Ideal Lattices**)**.** Let K be a number field of degree n, $R = \mathcal{O}_K$ and let σ be any additive injective map $\sigma : R \to \mathbb{C}^n$. Then the family of ideal lattices for the ring R and the embedding σ is the set of all lattices $\sigma(\mathcal{I})$ for integral ideals $\mathcal{I} \subset R$.

Remark 18. Let us now fix K to be the cyclotomic number field of degree $n = \phi(m)$, with m positive integer, which means that $R = \mathbb{Z}[x]/(\Phi_m(x))$. We

notice that by taking σ as the coefficient embedding, we get the definition of f-ideal lattices, with $f = \Phi_m$.

Whereas the protocols on ideal lattices we previously introduced take σ as the coefficient embedding, R-LWE uses the *canonical embedding*.

Embeddings. We know that given any number field $K = \mathbb{Q}(\zeta)$ of degree n we can consider n field homomorphisms $\sigma_i : K \to \mathbb{C}$ that fix any element of $\mathbb{Q}$ and map ζ to each of its conjugates. We indicate the number of real embeddings with s_1 and the number of pairs of complex embeddings with s_2, hence $n = s_1 + 2s_2$. Furthermore, we indicate with $\{\sigma_j\}_{j\in[s_1]}$ the real embeddings and we order the complex embeddings so that $\sigma_{s_1+s_2+j} = \overline{\sigma_{s_1+j}}$ for $j \in [s_2]$.

Definition 4.4 (**Canonical Embedding**)**.** The canonical embedding is the map $\sigma : K \to \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ defined as:

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_n(x)).$$

The canonical embedding is a field homomorphism from K to $\mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$, where both addition and multiplication are component-wise. In addition, due to the pairing of the complex embeddings, σ maps to H and furthermore, given an integral ideal $\mathcal{I}$ with $\mathbb{Z}$-basis $\{u_1, \dots, u_n\}$, we get an ideal lattice $\sigma(\mathcal{I}) \subset H$ with basis $\{\sigma(u_1), \dots \sigma(u_n)\}$. Hence, the lattices involved in our worst-case to average-case reduction are discrete subsets of H which are images of ideals of $R = \mathcal{O}_K$ under the canonical embedding. To sum up, by solving the SIVP for ideal lattices we mean to find short independent vectors for lattices of the kind $\sigma(\mathcal{I}) \subset H$, with $\mathcal{I} \in R$ integral ideal, where "short" is with respect to the norm induced on H by $\mathbb{C}^n$.
By identifying each element of $x \in K$ with its embedded $\sigma(x) \in H$, we can define the following norm on K using the one on H: for any $x \in K$ and any

$p \in [1, \infty]$, the l_p norm of x is:

$$\|x\|_p = \|\sigma(x)\|_p = (\sum_{i\in[n]} |\sigma_i(x)|^p)^{1/p} \qquad \text{for } p < \infty$$

$$\|x\|_\infty = \|\sigma(x)\|_\infty = \max_{i\in[n]} |\sigma_i(x)| \qquad \text{for } p = \infty$$

Furthermore, using the canonical embedding enables us to think the Elliptical Gaussian Distribution as a distribution over $K_\mathbb{R} \coloneqq K \otimes_\mathbb{Q} \mathbb{R}$: we can identify $K_\mathbb{R}$ with H and we define the distribution $D_\mathbf{r}$ of $x \otimes s \in K_\mathbb{R}$ as the distribution $D_{\mathbf{r}'}$ of $\sigma(x) \cdot s$ in H where $r_i^{'} = r_i \cdot |\sigma_i(x)|$, i.e. we sample $x \otimes s \in K_\mathbb{R}$ from $D_\mathbf{r}$ when $\sigma(x) \cdot s \in H$ is sampled from $D_{\mathbf{r}'}$.

4.1.3 Cyclotomic Number Fields and their properties

The second part of the hardness reduction for Ring-LWE relies on some properties of cyclotomic number fields. In this short section we briefly recall the concepts related to cyclotomic extensions that we are going to use in our search-to-decision equivalence. We now fix $K = \mathbb{Q}(\zeta)$, with $\zeta = \zeta_m = \exp(2\pi\sqrt{-1}/m)$, to be the mth cyclotomic field, $\Phi_m(x)$ the minimal polynomial of degree n and $R = \mathcal{O}_K = \mathbb{Z}[\zeta]$.

Prime Splitting. We now discuss the factorization of the ideal $\langle q \rangle$ for an integer prime $q \in \mathbb{Z}$. Let $\prod_i (f_i(x))^{e_i}$ be the factorization of $\Phi_m(x)$ over $\mathbb{Z}_q[x]$ into monic irreducible polynomials, then in R the factorization of $\langle q \rangle$ is $\langle q \rangle = \prod_i \mathfrak{q}_i^{e_i}$, with $\mathfrak{q}_i = \langle q, f_i(\zeta) \rangle$ prime ideal with norm $q^{deg(f_i)}$. As we will see later, we are going to work modulo a prime q such that $q = 1 \mod m$, thus we now focus on this specific case. Being cyclic of order $q-1$, the field $\mathbb{Z}_q$ has a primitive mth root of unity ω and actually each of the $n = \phi(m)$ distinct roots of unity ω^i, for $i \in \mathbb{Z}_m^*$, is in $\mathbb{Z}_q$. Thus, $\Phi_m(x)$ completely factors over $\mathbb{Z}_q[x]$ as $\prod_{i\in\mathbb{Z}_m^*}(x - \omega^i)$ and $\langle q \rangle$ splits completely into n distinct prime ideals $\langle q \rangle = \prod_{i\in\mathbb{Z}_m^*} \mathfrak{q}_i$, where $\mathfrak{q}_i = \langle q, \zeta - \omega^i \rangle$ has norm q. This particular factorization in distinct prime ideal $\mathfrak{q}_i$ with bounded norm will be extremely important in the search-to-decision reduction, as it will allow us to proceed

by enumeration in polynomial time.

Automorphisms. The cyclotomic field K has $n = \phi(m)$ automorphisms $(\tau_k)_{k\in\mathbb{Z}_m^*}$ defined as:

$$\begin{aligned} \tau_k \colon K &\to K \\ \zeta &\mapsto \zeta^k \end{aligned}$$

which are indeed automorphisms from $\mathbb{Q}(\zeta)$ to $\mathbb{Q}(\zeta^k) = \mathbb{Q}(\zeta)$. The following lemma follows directly from the fact that cyclotomic fields are Galois extensions of $\mathbb{Q}$(see [Ste04], Chapter 13 for a coincise proof).

Lemma 4.1.1. *In the same setting above, for any $i, j \in \mathbb{Z}_m^*$ we indicate with i^{-1} the multiplicative inverse of i in $\mathbb{Z}_m^*$ and thus with i/j the product ij^{-1} in $\mathbb{Z}_m^*$. Then for any $i, j \in \mathbb{Z}_m^*$, we have $\tau_j(\mathfrak{q}_i) = \mathfrak{q}_{i/j}$.*

4.1.4 Trace and Duality

The field trace $\mathrm{Tr} = Tr_{K/\mathbb{Q}} : K \to \mathbb{Q}$ of an element $x \in K$ is defined as the trace of the linear transformation on K representing the multiplication by x. In practice, the following properties can be shown:

- for any $x \in K$, $\mathrm{Tr(x)} = \sum_{i\in[n]} \sigma_i(x)$;
- Tr is additive;
- for any $x, y \in K$, $\mathrm{Tr}(x \cdot y) = \sum_{i\in[n]} \sigma_i(x) \cdot \sigma_i(y) = \langle \sigma(x), \overline{\sigma(y)} \rangle$.

Definition 4.5 (**Dual Ideal**)**.** For any fractional ideal $\mathcal{L} \in K$ (i.e. for the $\mathbb{Z}$-span of any $\mathbb{Q}$-basis of K), its dual is

$$\mathcal{L}^\vee = \{x \in K : \mathrm{Tr}(x\mathcal{L}) \subset \mathbb{Z}\}.$$

It is important to notice that the dual can be computed efficiently: given a fractional ideal $\mathcal{I}$ with $\mathbb{Q}$-basis $B = \{b_1, \ldots, b_n\}$, the dual basis $B^\vee =$

$\{b_1^\vee, \ldots, b_n^\vee\}$, characterized by $Tr(b_i \cdot b_j^\vee) = 1$ if $i = j$ and 0 otherwise, generates $\mathcal{I}^\vee$. In addition, for any $\mathbb{Q}$-basis B we have $(B^\vee)^\vee = B$, so any fractional ideal is self dual. An important and useful fact is the following relation concerning the inverse of any ideal $\mathcal{I}$, namely we have that $\mathcal{I}^\vee = I^{-1} \cdot R^\vee$. The case which we are going to deal with is precisely that of $R^\vee = \mathcal{O}_K^\vee$, which is a fractional ideal often called *codifferent*, whose inverse $(R^\vee)^{-1}$, the *different*, is an integral ideal.

4.1.5 Chinese Remainder Theorem

In this section we recall the Chinese remainder theorem for modules over $R = \mathcal{O}_K$, which we will use later in the search-to-decision reduction.

Theorem 4.1.2 (Chinese Remainder Theorem)**.** *Let $\mathcal{I}_1, \ldots, \mathcal{I}_r$ be pairwise coprime ideals in R, let A be an R-module and let $\mathcal{I} = \prod_{i\in[r]} \mathcal{I}_i$. The canonical R-module homomorphism $A \to \bigoplus_{i\in[r]}(A/\mathcal{I}_i A)$ induces an isomorphism of R-modules $A/\mathcal{I} \to \bigoplus_{i\in[r]}(A/\mathcal{I}_i A)$.*

4.2 The R-LWE problem and its variants

In this section we define the R-LWE Distribution and the two versions of the R-LWE problem. Ring-LWE is parametrized by a number field K with $R = \mathcal{O}_K$ and a prime modulus $q \geq 2$. We now define the problem in the most general way, allowing K to be any field extension even though the worst-case to average-case reduction for R-LWE has been proved only for cyclotomic fields. For any fractional ideal $\mathcal{J} \in K$, we set $\mathcal{J}_q = \mathcal{J}/q\mathcal{J}$ and we define $\mathbb{T} = K_\mathbb{R}/R^\vee$ with $R^\vee$ codifferent ideal.

Definition 4.6 (**Ring-LWE Distribution**)**.** Let $s \in R_q^\vee$ be the secret and ψ an error distribution over $K_\mathbb{R}$, then a sample from the ring-LWE distribution $A_{s,\psi}$ over $R_q \times \mathbb{T}$ is generated by choosing $a \leftarrow R_q$ uniformly random, $e \leftarrow \psi$ and outputting (a, $b = (a \cdot s)/q + e \mod R^\vee$).

Definition 4.7 (**Ring-LWE Search**(**R-LWE**$_{q,\Psi}$))**.** Let Ψ be a family of distributions over $K_{\mathbb{R}}$. The search version of ring-LWE is the following problem: given arbitrarily many independent samples from $A_{s,\psi}$, for some $s \in R_q^\vee$ and $\psi \in \Psi$, find s.

Definition 4.8 (**Average-Case Decision Ring-LWE**(**R-DLWE**$_{q,\Upsilon}$))**.** Let Υ be a distribution over a family of error distribution over $K_{\mathbb{R}}$. The average-case decision ring-LWE problem consists in dinstinguishing with non-negligible advantage between arbitrarily many independent samples from $A_{s,\psi}$, with $(s, \psi) \leftarrow U(R_q^\vee) \times \Upsilon$, and the same number of uniformly random and independent samples from $R_q \times \mathbb{T}$.

Before moving to the next section, we explicitely state what we intend by *non-negligible advantage*. If p is the probability that the adversary guesses correctly which of the two distributions has been used to generate the samples, then the **advantage** is defined as $|p - \frac{1}{2}|$. In practice, $\epsilon > 0$ is **non-negligible** if we have $\epsilon > 2^{-30}$.

4.2.1 Error Distributions

We now the introduce the family of error distributions we are using in the definitions above, i.e. the distributions for which the worst-case to average-case reduction effectively works. More precisely, **Definition 4.9** introduces the distribution we will use in R-LWE$_{q,\Psi}$, while **Definition 4.10** and **4.11** refer to the R-DLWE$_{q,\Upsilon}$ problem.

Definition 4.9 (**Family** $\Psi_{\leq\alpha}$)**.** Given $\alpha > 0$ real number, the family of error distributions $\Psi_{\leq\alpha}$ is the set of all elliptical Gaussian distributions $D_{\mathbf{r}}$ over $K_{\mathbb{R}}$ where for any parameter $\mathbf{r} = (r_1, \ldots, r_n)$ we have $r_i \leq \alpha$.

Definition 4.10 (**Gamma distribution** $\Gamma(2,1)$)**.** The gamma distribution $\Gamma(2,1)$ with shape parameter 2 and scale parameter 1 is the distribution with the following density:

$$f(x) = \begin{cases} xe^{-x} & \text{for } x \geq 0 \\ 0 & \text{for } x < 0 \end{cases}$$

Definition 4.11 (**Distribution Υ_α**)**.** Let α be a positive real number, then a distribution sampled from Υ_α is an elliptical Gaussian distribution $D_{\mathbf{r}}$ over $K_{\mathbb{R}}$ whose parameters $r_i > 0$ are such that $r_i^2 = r_{i+n/2}^2 = \alpha^2(1 + \sqrt{n}x_i)$, with $x_1, \ldots, x_n$ chosen independently from $\Gamma(2, 1)$.

4.3 Hardness

As in the case of the LWE problem, the reduction from the R-LWE to some lattice problem in the worst-case involves quantum computing. After stating the main theorem of [LPR12], we discuss the structure of its proof and we finally focus on the Decision-to-Search reduction.

Theorem 4.3.1. *Let K be the mth cyclotomic number field with dimension $n = \phi(m)$ and let $R = \mathcal{O}_K$ be its ring of integers. Let $\alpha = \alpha(n) > 0$ 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 $\tilde{O}(\sqrt{n}/\alpha)$-approximate SIVP over ideal lattices to R-DLWE$_{q,\Upsilon_\alpha}$.*

The proof is made up by two different parts which are essentially independent:

Worst-case hardness of the search problem. In this component it is proved that, for a specific choice of of parameters, the R-LWE$_{q,\Psi}$ is at least as hard as quantumly solving SIVP$_\gamma$ on ideal lattices of R. It is important to notice that this reduction actually works in any number field, not only for cyclotomic ones.

Decision-to-Search reduction In this part it is shown that solving the decision version of the R-LWE is at least as hard as solving its search variant; thus if SIVP$_\gamma$ is hard to solve in the quantum setting, then the Ring-LWE Distribution is pseudorandom. It is important to remark that this reduction

is entirely classical. Furthermore, this component relies on specific properties of cyclotomic number fields, such as being Galois, and on the particular choice of modulus q, namely that $\langle q \rangle$ splits completely into n prime ideals $\mathfrak{q}_i$ which are permuted transitively by the automorphisms of the Galois group (see 4.1.3).

4.3.1 Hardness of Search-LWE

Theorem 4.3.2. *Let K be an arbitrary number field of degree n and $R = \mathcal{O}_K$. Let $\alpha = \alpha(n) > 0$ and let $q = q(n) \geq 2$ be such that $\alpha q \geq \omega(\sqrt{\log n})$. Then there is a probabilitic polynomial-time quantum reduction from $\tilde{O}(\sqrt{n}/\alpha)$-approximate SIVP to R-LWE$_{q,\Psi_{\leq\alpha}}$, where $\gamma = \eta_\epsilon(\mathcal{I}) \cdot \omega(\sqrt{\log n}/\alpha)$ for some negligible $\epsilon = \epsilon(n)$.*

This reduction follows the idea of Regev's proof[Reg05] for general lattices, and works by applying repeatedly an iterative step whose goal is to find shorter and shorter vectors. Up to now, quantum computing does not seem to be replaceable by any classical tecniques and it is needed in order to have polynomial-time iterative steps.

4.3.2 Hardness of Decision-LWE

In this section we are going to show that for the errors distributions defined above and for a particular choice of parameters and ring, the Decision-LWE is hard to solve, i.e. the ring-LWE distribution is pseudorandom. From now on we restrict to the setting of **Theorem 4.3.1**, so we fix the following notations: $\zeta = \zeta_m$ is a primitive mth root of unity, $K = \mathbb{Q}(\zeta)$ is the mth cyclotomic number field with dimension $n = \phi(m)$, $R = \mathcal{O}_K = \mathbb{Z}[\zeta]$ its ring of integer, $R^\vee$ its codifferent and $q = 1 \mod m$ is a poly(n)-bounded prime. We finally recall that we discussed the behaviour of $\langle q \rangle$ and of the automorphisms of $\mathbb{Q}(\zeta)$ in 4.1.3.
The following theorem gives us the reduction from the search version of R-LWE (whose hardness derives from **Theorem 4.3.2**) to R-DLWE$_{q,\Upsilon_\alpha}$

Theorem 4.3.3. *Let R and q be as above and let $\alpha q \geq \eta_\epsilon(R^\vee)$ for some negligible $\epsilon = \epsilon(n)$. Then there is a randomized polynomial-time reduction from R-LWE$_{q,\Psi_{\leq\alpha}}$ to R-DLWE$_{q,\Upsilon_\alpha}$.*

The proof of the theorem above consists of a concatenation of 4 different and independent reductions, whose extremes are the search and the decision version of R-LWE. The sequence is represented below and all the intermediate problems will be defined later. Each right arrow represents a reduction, i.e. knowing how to solve the problem which is pointed to allows us to solve the previous one. In addition, the number above each arrow is the number of the corresponding lemma .

$$\textbf{R-LWE}_{q,\Psi} \xrightarrow{4.3.5} \mathfrak{q}_i\textbf{-LWE} \xrightarrow{4.3.6} \textbf{WDLWE}^i_{q,\Psi} \xrightarrow{4.3.7} \textbf{DLWE}^i_{q,\Upsilon} \xrightarrow{4.3.9} \textbf{DLWE}_{q,\Upsilon}$$

4.3.2.1 Search to Worst-case Decision

In this part we consider the first two reductions, namely we reduce the search version of R-LWE$_{q,\Psi_{\leq\alpha}}$ to a particular decision problem relative to just one arbitrarily prime ideal $\mathfrak{q}_i$. Both this last problem and the intermediate one are worst-case problems over the choice of $s \in R_q^\vee$ and $\psi \in \Psi_{\leq\alpha}$, hence the worst-case to average-case reduction will be dealt with in the next section. The first intermediate problem can be viewed as a local variant of R-LWE, and it is defined as follows.

Definition 4.12 (**LWE over $\mathfrak{q}_i$** ($\mathfrak{q}_i$-LWE))**.** Given access to $A_{s,\psi}$ for some arbitrary $s \in R_q^\vee$ and $\psi \in \Psi_{\leq\alpha}$ for some $\alpha > 0$, find $s \mod \mathfrak{q}_i R^\vee$.

Lemma 4.3.4. *For any $\alpha > 0$, the family $\Psi_{\leq\alpha}$ is closed under every automorphism τ of K, i.e. $\psi \in \Psi_{\leq\alpha} \Rightarrow \tau(\psi) \in \Psi_{\leq\alpha}$.*

Proof. Let $\tau_j : K \to K$ be any automorphism of K, then we know that $\tau_j(\zeta) = \zeta^j$ for some $j \in \mathbb{Z}_m^*$. Consider now $i \in \mathbb{Z}_m^*$ and any ζ^k of the power basis of K, then $\sigma_i(\zeta^k) = (\zeta^k)^i = (\zeta^{kj})^{i/j} = \sigma_{i/j}(\tau_j(\zeta^k))$ which means that for any $x \in K$ the coordinates of $\sigma(x) \in H$ and $\sigma(\tau_j(x)) \in H$ are a rearrangement of each other. □

Lemma 4.3.5 (R-LWE to $\mathfrak{q}_i$-LWE)**.** *For every $i \in \mathbb{Z}_m^*$ there is a deterministic polynomial-time reduction from R-LWE$_{q,\Psi_\alpha}$ to $\mathfrak{q}_i$-LWE$_{q,\Psi_\alpha}$.*

Proof. The idea of the proof is the following: we combine the oracle for $\mathfrak{q}_i$-LWE and the field automorphism τ_k to get $s \mod \mathfrak{q}_j R^\vee \ \forall j \in \mathbb{Z}_m^*$, then we use the Chinese Remainder Theorem to reconstruct $s \in R_q^\vee$. We transform each sample $(a, b) \leftarrow A_{s,\psi}$ into the sample $(\tau_k(a), \tau_k(b)) \in R_q \times \mathbb{T}$ with $k = j/i \in \mathbb{Z}_m^*$ and thus $\tau_k(\mathfrak{q}_j) = \mathfrak{q}_i$. Then we give our new samples to the oracle of $\mathfrak{q}_i$-LWE$_{q,\psi}$ and if its answer is $t \in R^\vee/\mathfrak{q}_i R^\vee$ we return $\tau_k^{-1}(t) \in R^\vee/\mathfrak{q}_j R^\vee$, since $\tau_k^{-1} = \tau_{k^{-1}}$. We now prove that $\tau_k^{-1}(t) = s \mod \mathfrak{q}_j R^\vee$: for each original sample $(a, b) \leftarrow A_{s,\psi}$, since $b = as/q + e \mod R^\vee$ and $\tau_k(q) = q$, we have

$$\tau_k(b) = \tau_k(a) \cdot \tau_k(s)/q + \tau_k(e) \mod R^\vee.$$

In addition, since τ_k is an automorphism on R, $\tau_k(a)$ is uniformly random in $\tau_k(R_q)$ and the samples $(\tau_k(a), \tau_k(b))$ are distributed according to $A_{\tau_k(s),\psi'}$ with $\psi' = \tau_k(\psi) \in \Psi$ by **Lemma 4.3.5**. Our original oracle therefore output $t = \tau_k(s) \mod \mathfrak{q}_i R^\vee$ so $\tau_k^{-1}(t) = s \mod \tau_k^{-1}(\mathfrak{q}_i R^\vee) = s \mod \mathfrak{q}_j R^\vee$. □

Before going into the second reduction, we introduce the following notations: we identify the elements of $\mathbb{Z}_m^*$ with their integer representatives in $\{1, \ldots, m-1\}$ and for each $i \in \mathbb{Z}_m^*$ we denote with $i-$ the largest element in $\mathbb{Z}_m^*$ less than i, with the convention that $1- = 0$.

Definition 4.13 (**Hybrid LWE Distribution**)**.** For $i \in \mathbb{Z}_m^*$, $\mathbf{s} \in R_q^\vee$ and ψ error distribution over $K_\mathbb{R}$, the distribution $A_{s,\psi}^i$ over $R_q \times \mathbb{T}$ is defined in the following way: choose $(a, b) \leftarrow A_{s,\psi}$ and output $(a, b + r/q)$ with $r \in R_q^\vee$ such that:

- r is uniformly random and independent $\mod \mathfrak{q}_j R^\vee$ for any $j \leq i$;
- r is $0 \mod \mathfrak{q}_j R^\vee$ for all $j > i$.

In addition we define $A_{s,\psi}^0 \coloneqq A_{s,\psi}$.

Definition 4.14 (**Worst-case decision $\mathfrak{q}_i$-LWE($\mathbf{WDLWE}^i_{q,\Psi}$)).** For $i \in \mathbb{Z}_m^*$ and a family of distributions Ψ, the $\mathrm{WDLWE}^i_{q,\Psi}$ is defined as follows: given access to $A^j_{s,\psi}$ for arbitrary $s \in R_q^\vee$, $\psi \in \Psi$ and $j \in \{i-, i\}$, find j.

Lemma 4.3.6 (Search to Decision)**.** *For any $i \in \mathbb{Z}_m^*$ there is a probabilistic polynomial-time reduction from $\mathfrak{q}_i$-LWE$_{q,\Psi}$ to WDLWE$^i_{q,\Psi}$.*

Proof. The idea to get $s \mod \mathfrak{q}_i R^\vee$ is to test each of its possible value: we modify the samples we receive according to the value we are considering so that on the correct one the modified samples are distributed according to $A^{i-}_{s,\psi}$, while on the remaining values these samples are distributed according to $A^i_{s,\psi}$. Finally, by using the oracle for $\mathrm{WDLWE}^i_{q,\Psi}$ we can discover which distribution was generated. We underline that since we have only $\mathrm{N}(\mathfrak{q}_i) = q = poly(n)$ possible values for $s \mod \mathfrak{q}_i R^\vee$, we can enumerate over them efficiently.
We define now the transformation that given $g \in R_q^\vee$ modifies the distribution $A_{s,\psi}$ in either $A^i_{s,\psi}$ or $A^{i-}_{s,\psi}$ according to wether $g = s \mod \mathfrak{q}_i R^\vee$ or not. Given $(a, b) \leftarrow A_{s,\psi}$, we consider the sample

$$(a', b') = (a + v, b + (r + vg)/q)) \in R_q \times \mathbb{T}, \quad \text{with:}$$

- $v \in R_q$ uniformly random $\mod \mathfrak{q}_i$ and $0 \mod \mathfrak{q}_j$ for all $j \neq i$;
- $r \in R_q^\vee$ uniformly random and independent $\mod \mathfrak{q}_j R^\vee$ for all $j < i$ and $0 \mod \mathfrak{q}_j R^\vee$ for $j \geq i$.

We now notice that since a is uniformly random in R_q, so is a'. In addition, we can write b' as:

$$\begin{aligned} b' = b + (r + vg)/q &= (as + r + vg)/q + e \\ &= (a's + r + v(g - s))/q + e, \end{aligned}$$

with $e \leftarrow \psi$.
Suppose we have $g = s \mod \mathfrak{q}_i R^\vee$, then for all $k \in \mathbb{Z}_m^*$ we have $v(g-s) = 0 \mod \mathfrak{q}_k R^\vee$ and hence by the Chinese remainder theorem $v(g-s) = 0 \in R_q^\vee$.

Hence the distribution of (a', b') is $A^{i-}_{s,\psi}$: a' is uniformly random over R_q, while $b' = (a's)/q + r/q + e \mod \mathfrak{q}_j R^\vee$ with $r \in R_q^\vee$ uniformly random and independent for all $j < i$ and $0 \mod$ all the remaining $\mathfrak{q}_j R^\vee$.
Now, assume that $g \neq s \mod \mathfrak{q}_i R^\vee$. Then since $\mathfrak{q}_i$ is a maximal ideal (prime in R), $R^\vee/\mathfrak{q}_i R^\vee$ is a field and hence $v(g-s)$ is uniformly random $\mod \mathfrak{q}_i R^\vee$. In addditon, $v(g-s)$ is 0 mod all other $\mathfrak{q}_j R^\vee$ by the definition of v and hence the distribution of (a', b') is $A^{i}_{s,\psi}$: a' is uniformly random over R_q, while $b' = (a's)/q + (v(g-s)+r)/q$ with $v(g-s)+r$ uniformly random and independent $\mod \mathfrak{q}_j R^\vee$ for all $j \leq i$, and $0 \mod$ all the remaining $\mathfrak{q}_j R^\vee$. □

4.3.2.2 Worst-Case to Average-Case Decision

To conclude present the last two reductions which will bring us to the $\mathrm{DLWE}_{q,\Upsilon_\alpha}$. Since we start from $\mathrm{WDLWE}^i_{q,\Psi}$, which is a *local* worst-case problem, first we move to an average-case local problem, then we remove the dependence on a specific $\mathfrak{q}_i$. A proof of the first reduction can be found in [LPR12].

Definition 4.15 (**Average-case decision $\mathfrak{q}_i$-LWE**($\mathrm{DLWE}^i_{q,\Upsilon}$))**.** For any $i \in \mathbb{Z}_m^*$ and Υ distribution over error distributions, an algorithm solves the $DLWE^i_{q,\Upsilon}$ if over random choices $(s, \psi) \leftarrow U(R_q^\vee) \times \Upsilon$, it distinguishes with non-negligible advantage inputs from $A^i_{s,\psi}$ versus inputs from $A^{i-}_{s,\psi}$

Lemma 4.3.7 (Worst-Case to Average-Case)**.** *For any $\alpha > 0$ and any $i \in \mathbb{Z}_m^*$, there is a randomized polynomial-time reduction from $WDLWE^i_{q,\Psi_{\leq\alpha}}$ to $DLWE^i_{q,\Upsilon_\alpha}$*

We now state a lemma we are going to use in our last reduction to $\mathrm{DLWE}_{q,\Upsilon}$.

Lemma 4.3.8. *Let $\alpha \geq \eta_\epsilon(R^\vee)/q$ for some $\epsilon > 0$. Then for any ψ in the support of $\Psi_{\leq\alpha}$ and $s \in R_q^\vee$, the distribution $A^{m-1}_{s,\psi}$ is within statistical distance $\epsilon/2$ from the uniform distribution over $(R_q, \mathbb{T})$.*

Lemma 4.3.9. *Let Υ be a distribution over a family of error distributions such that for any ψ in the support of Υ and any $s \in R_q^\vee$ the distribution $A_{s,\psi}^{m-1}$ is within negligible statistical distance from the uniform. Then for any oracle solving the $DLWE_{q,\Upsilon}$ problem, there exist an $i \in \mathbb{Z}_m^*$ and an efficient algorithm that solves $DLWE_{q,\Upsilon}^i$ using this oracle.*

Proof. Let (s, ψ) be any pair for which the oracle distinguish between samples from $A_{s,\psi}$ and the uniform distribution with non-negligible advantage. Since $A_{s,\psi}^0 = A_{s,\psi}$ and $A_{s,\psi}^{m-1}$ is negligibly far from the uniform distribution, for each such (s, ψ) there must be an $i \in \mathbb{Z}_m^*$ for which the oracle distinguish between $A_{s,\psi}^i$ and $A_{s,\psi}^{i-}$ with non-negligible advantage. Hence, fixing this i we can solve $DLWE_{q,\Upsilon}^i$ and the lemma follows. □

Chapter 5

Open Questions

In this final chapter we formally describe some open problems of lattice-based cryptography. We will notice that many of these questions stem straighforwardly from previous remarks or already stated conjectures.

Problems on Ideal Lattices. For worst-case problems on ideal lattices, in particular those of cyclotomic rings, are there classical or quantum algorithms that outperform the known ones for general lattices? If so, can these algorithms be used to solve the R-LWE?

Hardness of NTRU. Despite being very secure in practice, we know that no theoretical proof of NTRU's hardness has been developed yet. Is it possible to find a worst-case to average-case reduction for this specific problem?

Classical Hardness of LWE. Up to now, besides Regev's quantum reduction, the only entirely classical worst-case to average case-reduction regarding LWE presents the consistent drawback of the size of the modulus q (see *Remark 15*). Is it possible to overcome this problem?

Classical Hardness of R-LWE. The reduction we presented, due to Lyubashesky, Peikert and Regev, relies on quantum computing. Is it possi-

ble to get a classical worst-case hardness reduction for R-LWE? If not, can we get at least a partial dequantization as for LWE?

R-LWE in arbitrary fields. We know that the worst-case reduction for the search version of R-LWE works in arbitrary number fields, while the decision to search reduction relies on properties of Galois extensions, namely their automorphisms. Hence it is natural to wonder if there is an analogue proof of the hardness of the decisional version of R-LWE which might work for any number field.

Bibliography

[Ajt96a] M. Ajtai. *Generating hard instances of lattice problems.* STOC, 1996.

[Ajt96b] M. Ajtai. *Representing hard lattices with O(n* $\log n$*) bits.* STOC, pages 94-103, 1996.

[Ajt05] M. Ajtai *Representing hard lattices with O(n*log *n) bits.* Proceedings 37th Annual ACM Symposyum of Computing (STOC), 2005.

[AD97] M. Ajtai and C. Dwork. *A public-key cryptosystem with worst-case/average-case equivalence.* STOC, pages 284-293, 1997.

[AD15] M. Ajtai and C. Dwork. *The first and fourth public-key cryptosystem with worst-case/average-case equivalence.* STOC, pages 733-742, 2015.

[AKS01] M. Ajtai, R. Krumar and D. Sivakumar. *A sieve algorithm for the shortest lattice vector problem.* STOC, pages 601-610, 2001.

[Boy10] X. Boyen. *Lattice mixing and vanishing trapdors: A framework for fully secure short signatures and more.* Public Key Cryptography, pages 499-517, 2010.

[BGV14] Z. Brakerski, C. Gentry and V. Vaikuntanathan. *Leveled fully homomorphc encryption without bootstrapping.* TOCT, 6(3):13, 2014.

[BV12] Z. Brakerski and V. Vaikuntanathan. *Efficient fully homomorphic encryption from ring-LWE and security for key dependent messages0.* CRYPTO, pages 868-886, 2012.

[CHK09] D. Cash, D. Hofheinz and E. Kiltz. *How to delegate a lattice basis.* Cryptology ePrint Archive, Report 2009/351, July 2009. Available at *http://eprint.iacr.org/.*

[CMNT11] J.-S. Coron, A. Mandal, D. Naccache and M. Tibouchi. *Fully homomorphic encryption over the integers with shorter public keys..* CRYPTO, pages 487-504, 2011.

[Con09] K.Conrad. *The different ideal.* Available at *http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/different.pdf.*

[CN97] J.-Y. Cay and A. Nerurkar. *An improved worst-case to average-case connection for lattice problems.* FOCS, pages 468-477, 1997.

[DWA15] D-WAVE. *D-Wave Systems Announces the General Availability of the 1000+ Qubit D-Wave 2X Quantum Computer.* Available at *http://www.dwavesys.com/press-releases/d-wave-systems-announces-general-availability-1000-qubit-d-wave-2x-quantum-computer.*

[Gen09a] C. Gentry. *A fully homomorphic encryption scheme.* Ph.d thesis, Stanford, 2009.

[Gen09b] C. Gentry. *Fully homomorphic encryption using ideal lattices.* STOC, pages 169-178, 2009.

[GPV08] C. Gentry, C. Peikert and V. Vaikuntanathan. *Trapdoors for hard lattices and new cryptographic constructions.* STOC, pages 197-206, 2008.

[GSW13] C. Gentry, A. Sahai and B. Waters. *Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based.* CRYPTO, pages 75-92, 2013.

[HPS98] J. Hoffstein, J. Piper and J.H. Silverman. *NTRU: A ring-based public key cryptosystem.* ANTS, pages 267-288, 1998.

[HPS01] J. Hoffstein, J. Piper and J.H. Silverman. *NSS: an NTRU lattice-based signature scheme.* EUROCRYPT, pages 211-228, 2001.

[IBM15] IBM. *IBM Scientists Achieve Critical Steps to Building First Practical Quantum Computer.* Available at *http://www-03.ibm.com/press/us/en/pressrelease/46725.wss*

[KTX08] A. Kawachi, K. Tanaka and K. Xagawa. *Concurrently secure identification schemes based on the worst-case hardness of lattice problems.* ASIACRYPT, pages 372-389, 2008.

[Kan83] Ravi Kannan. *Improved Algorithms for integer programming and related lattice problems.* STOC pages 193-206, 1983.

[LLL82] A.K. Lenstra, H.W. Lenstra and L. LovÃ sz. *Factoring polynomial with rational coefficients.* Mathematische Annalen, n. 261, pages 515-534, December 1982.

[LM06] V. Lyubashevsky and D. Micciancio. *Generalized compact knapsacks are collision resistant.* 33rd International Colloquium on Automata, Languages and Programming (ICALP), 2006.

[LM09] V. Lyubashevsky, D. Micciancio. *On bounded distance decoding, unique shortest vectors, and the minimum distance problem.* CRYPTO, pages 577-594, 2009.

[LMP12] V. Lyubashevsky, D. Micciancio, C. Peikert and A. Rosen. *SWIFTT: A modest proposal for FFT hashing.* FSE, pages 54-72,2012.

[LPR12] V. Lyubashevsky, C. Peikert and O. Regev *On ideal lattices and learning with errors over rings.* Journal of the ACM, 60(6):43:1-43:35, 2012.

[LPR13] V. Lyubashevsky, C. Peikert and O. Regev *A toolkit for Ring-LWE cryptography.* Available at *www.di.ens.fr/ lyubash/papers/toolkit.pdf.*

[Lyu08] V. Lyubashevsky. *Lattice-based identification scheme secure under active attacks.* Publick Key Cryptography, pages 162-179, 2008.

[MG12] D. Micciancio, S. Goldwasser. *Complexity of lattice problems.* Springer, 2012.

[Mic04] D. Micciancio. *Almost perfect lattices, the covering radius problem, and application to Ajtai's connection factor.* SIAM Journal Comput., 34(1)118-169, 2004.

[Mic07] D. Micciancio. *Generalized compact knapsacks, cyclic lattices, and effiient one-way function from worst-case complexity assumptions.* Computational Complexity, 16(4): 365-411, 2007.

[MP12] D. Micciancio and C. Peikert. *Trapdoors for lattices: Simpler, tighter, faster, smaller.* EUROCTYPT, 2012.

[MP13] D. Micciancio and C. Peikert. *Hardness of SIS and LWE with small parameters.* CRYPTO, pages 21-39, 2013.

[MR07] D. Micciancio and O. Regev. *Worst-case to average-case reductions based on Gaussian measures.* SIAM Journal Comput., 37(1)267-302, 2007.

[MR09] D. Micciancio and O. Regev. *Lattic-based cryptography.* Post Quantum Cryptography, pages 147-191. Springer, February 2009. bibitem[MV03]K91 D. Micciancio and S.P. Vadhan. *Statistcal zero-knowledge proofs with efficient provers: Lattice problems and more.* CRYPTO, pages 282-298, 2003.

[MV10] D.Micciancio and P. Voulgaris. *A deterministic single sxponential time alagorithm for most lattice problems based oon Voronoi cell computations.* Stoc, pages 351-358, 2010.

[Nit11] A. Nitaj. *Quantum and Post Quantum Cryptography.* Available at *http://www.math.unicaen.fr/ nitaj.*

[NS98] P. Q. Nguyen and J. Stern. *Cryptoanalysis of the Ajtai-Dwork cryptosystem*. CRYPTO, pages 223-242, 1998.

[NSA15] NSA. *http://www.nsa.gov/ia/programs/suiteb_cryptography*

[Orl15] B. Orlin. Blog: *https://mathwithbaddrawings.com/*

[Pei09a] C. Peikert *Public-key cryptosystems from the worst-case shortest vector problem*. STOC, pages 333-342, 2009.

[Pei09b] C. Peikert. *Bonsai trees (or, arboriculture in lattice-based cryptography)*. Cryptology ePrint Archive, Report 2009/359, July 2009. Available at *http://eprint.iacr.org/*.

[Pei15] Chris Peikert. *A Decade of Lattice Cryptography*. Cryptology ePrint Archive: Report 2015/939, September 26, 2015, available at *https://eprint.iacr.org/2015/939.pdf*

[PR06] C. Peikert and A. Rosen *Efficient collision resistant hashing from worst-case assumptions on cyclic lattices*. 3rd Theory of Cryptographic Conference (TCC), pages 145-166, 2006.

[PW08] C. Peikert and B. Waters. *Lossy trapdoor functions and their applications*. STOC, pages 187-196, 2008.

[Reg05] O. Regev *On lattices, learning with errors, random linear codes, and cryptography*. J. ACM 56(6):1-40, 2009. Preliminary version in STOC, 2005.

[Reg10] O. Regev *The learning with errors problem*. IEEE Conference on Computational Complexity, pages 191-204, 2010.

[RAD78] R.L Rivest, L.Adleman, M.L. Dertouzos. *On data banks and private homomorphisms*. Foundations of secure computations, 4(11):169-180, 1978.

[Sch87] C. Schnorr. *A hierarchy of polynomisl time lattice basis reduction algorithms.* Theoretical Computer Science Journal, n.53, pages 201-224, 1987.

[Sho97] P.W. Shor. *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.* SIAM J. Comput., 26(5)1484-1509, 1997.

[Ste04] W. Stein. *A Brief Introduction to Classical and Adelic Algebraic Number Theory.* Available at *http://wstein.org/129/ant/ant.pdf*

[SS11] D. Stehlé and R. Steinfeld. *Making NTRU as secure as worst-case problem over ideal lattices.* EUROCRYPT, pages 27-47, 2011.