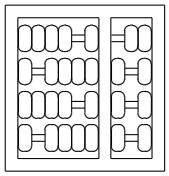

INSTITUTO DE COMPUTAÇÃO
UNIVERSIDADE ESTADUAL DE CAMPINAS

Lattice-based cryptography

Eduardo Morais

Ricardo Dahab

Technical Report - IC-2016-1 - Relatório Técnico

April - 202016 - Abril

Lattice-based cryptography

Eduardo Morais

Ricardo Dahab

April, 2016

Abstract

In this document we will give an introduction to lattice-based cryptography. Some mathematical apparatus will be presented to the reader and the main concepts are going to be pointed out. We will show how cryptography can be constructed under the assumption that a determined lattice problem is hard and we will see that it is possible to add algebraic structure to the subjacent lattice in order to obtain more efficient cryptosystems. Recently, new primitives have emerged, showing that lattice-based cryptography can achieve flexibility and malleability, while improvements in the performance have shown that it is becoming a practical possibility for some scenarios.

1 Introduction

Recently, lattice-based cryptography has been an important topic in the cryptographic community. Among the reasons that explain this fact, we remark that some hard problems over lattices have the special property of allowing ***worst-case reductions***. It means that cryptosystems can be proved to be secure on average based on the assumption that some lattice problem is hard in the worst-case. In other words, we can generate parameters and keys to our cryptographic scheme using a determined probability distribution in such an way that any adversary that breaks the

security of the scheme can be used as a black-box to solve ***any*** instance of a certain lattice problem. Another important fact about lattice-based cryptography is that it resists against ***quantum attacks***, i. e. attacks that have access to quantum computers. Hence lattice-based cryptography is part of the ***post-quantum cryptography***. Finally, lattices can be used to construct new cryptographic primitives, as for example ***fully homomorphic encryption*** [Gen09], that is an encryption scheme that produces malleable ciphertexts that can be algebraically manipulated allowing the construction of very flexible cryptosystems. The main goal of this document is to introduce the reader to the subject and present the mathematical background necessary to understand some details involved in the design and implementation of secure lattice-based cryptography.

1.1 Organization

In Section 2 we describe basic facts about abstract algebra. In Section 3 we give the main definitions and theorems and describe the hard problems over lattices. In Section 4 we present some cryptographic primitives that can be constructed based on these problems. In Section 5 we briefly describe other applications that can be achieved using lattices.

2 Abstact Algebra

In this section we give basic abstract algebra definitions and theorems. We also define homomorphisms, which is a central figure not only in the study of algebra, but also in lattice-based cryptography. For further information on this subject, we point the reader to Dummit and Foot's book [DF03].

2.1 Groups

Definition 2.1. A ***group*** is defined by the pair $(G, \circ)$, where $\circ$ is a ***closed associative binary operation*** over a set G, that contains an ***identity element***. Furthermore, every element from G has ***inverse*** in G. If the group respects the ***commutative property*** it is called ***Abelian*** group.

Example 2.1. The set of integer numbers $\mathbb{Z}$ and the addition operation forms an Abelian group, whose identity element is 0. Each element $a \in \mathbb{Z}$ has inverse given by $-a \in \mathbb{Z}$. The set of non-zero real numbers $\mathbb{R}$ with usual multiplication forms an Abelian group, whose identity is 1. Each element $a \in \mathbb{R}$ has inverse given by $1/a \in \mathbb{R}$. Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Given $a, b \in \mathbb{Z}_n$, we define the operations $\oplus$ and $\odot$ as follows:

$$\begin{aligned} a \oplus b &= a + b \pmod{n} \\ a \odot b &= a.b \pmod{n}. \end{aligned}$$

Thus, $(\mathbb{Z}_n, \oplus)$ forms an Abelian group, whose identity is again 0. Each element $a \in \mathbb{Z}_n$ has inverse given by $(n - a) \in \mathbb{Z}_n$. Moreover, let $\mathbb{Z}_n^* = \{1, \ldots, n-1\}$. Then $(\mathbb{Z}_n^*, \odot)$ forms a Abelian group if and only if n is a prime number. The multiplicative inverse $a \in \mathbb{Z}_n^*$ can be computed solving the Diophantine equation $a.x + n.y = 1$. As this equation has only one solution modulo n if $\mathrm{GCD}(a, n) = 1$, we have that, for a non-prime n, the elements $a \in \mathbb{Z}_n^*$ that have no inverses are such that $\mathrm{GCD}(a, n) \neq 1$. As long as there is no ambiguity, the symbols $+$ and $.$ are used instead of $\oplus$ and $\odot$, respectively.

Example 2.2. Let $\mathbb{Z}$ be the group defined in example 2.1 and $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$, formed by the addition of each element of $\mathbb{Z}$ with itself, obtaining the set of even numbers. Then $2\mathbb{Z}$ is the subgroup of $\mathbb{Z}$, because given two elements $a, b \in 2\mathbb{Z}$, $a + b$ is an even number, hence it belongs to $\mathbb{Z}$. Moreover, given an element of $a \in 2\mathbb{Z}$, there is $-a \in \mathbb{Z}$, such that $-a$ is the inverse of a.

2.1.1 Quotient group

Definition 2.2. Given a group $(G, \circ)$, a subgroup H and $a \in G$, we define the ***left coset*** as the set given by $a \circ H = \{a \circ h \mid h \in H\}$. Analogously, we define the ***right coset*** as the set given by $H \circ a = \{h \circ a \mid h \in H\}$.

If G is an Abelian group, then $a \circ H = H \circ a$ and hence there is no difference between left cosets and right cosets.

Theorem 2.1. Let H be a subgroup of G. Then the order of H divides the order of G.

Proof. It is easy to see that if $a \notin H$, then $a \circ H \cap H = \{\oslash\}$, because otherwise we would have $a \circ h_1 = h_2$, for $h_1, h_2 \in H$. Thus $a = h_2 \circ h_1^{-1}$ and hence $a \in H$, establishing a contradiction. Moreover, $|a \circ H| = |H|$, because otherwise we would have distinct elements $h_1, h_2 \in H$, such that $a \circ h_1 = a \circ h_2$, but this implies that $a^{-1} \circ a \circ h_1 = a^{-1} \circ a \circ h_2$ and then we have that $h_1 = h_2$, a contradiction. Thus, G can be partitioned in cosets derived from H. Namely, $G = H \cup a_1 \circ H \cup \cdots \cup a_k \circ H$, where a_i does not belong to H and also does not belong to no other coset $a_j \circ H$, para $i \neq j$.

Therefore, $|G| = (k+1).|H|$. □

Definition 2.3. The ***quotient group*** G/H is defined as being formed by equivalence classes generated by the partitioning of G with respect to H. If this partitioning is given by $\{H, a_1 \circ H, \ldots, a_k \circ H\}$, the operation $\star$ over the quotient group is defined by

$$(a_i \circ H) \star (a_j \circ H) = (a_i \circ a_j) \circ H.$$

Corolary 2.1. $|G/H| = |G|/|H|$.

For example, the quotient group $\mathbb{Z}/n\mathbb{Z}$, denoted also by $\mathbb{Z}_n$, is formed by the cosets:

$$\begin{aligned} n\mathbb{Z} &= \{0, n, 2n, \dots\}, \\ n\mathbb{Z}+1 &= \{1, n+1, 2n+1, \dots\}, \\ &\vdots \\ n\mathbb{Z}+(n-1) &= \{n-1, 2n-1, 3n-1, \dots\}. \end{aligned}$$

2.1.2 Homomorphisms

Definition 2.4. The function $f : G \to H$ is called ***homomorphism*** from G to H, if f preserves operations of group G. In other words, if $\circ$ and $\star$ are the operations of G and H respectively, then we say that f preserves the operation of G if for any $a, b \in G$, then $f(a \circ b) = f(a) \star f(b)$. If f is a bijection, then f is denominated ***isomorphism***. If f is a bijection from G to G, then f is called ***automorphism***.

Theorem 2.2. Let $f : G \to H$ be a homomorphism between groups G and H. If $e \in G$ represents the identity element of G, then $f(e)$ represents the identity of H.

Proof. Using the definition of homomorphisms together with the fact that $e.e = e$, we have $f(e).f(e) = f(e)$. Therefore, $f(e)$ is the identity element of H. □

Theorem 2.3. Let $f : G \to H$ be a homomorphism between the groups G and H. Then f maps inverses from G to inverses of H. In other words, for every $a \in G$, we have that $f(a^{-1}) = (f(a))^{-1}$.

Proof. For any $a \in G$, we have that $a.a^{-1} = e$. Thus, $f(a)f(a^{-1}) = f(e)$. Hence, $f(a^{-1}) = (f(a))^{-1}$. □

Example 2.3. An important example of automorphism of a group G, called ***inner automorphism***, is the provided by conjugation by a fixed element in G. Namely, $f_a : G \to G$, such that, for any $a \in G$, then $f_a(x) = axa^{-1}$. Then elements x and axa^{-1} are called ***conjugates***. Given a subgroup S of G, the set $aSa^{-1} = \{asa^{-1} \mid s \in S\}$, for $a \in G$, is denominated ***conjugate*** of a subgroup S.

Let $f : G \to H$ be a homomorphism from G to H. The set $N = \{a \mid f(a) = e'\}$, where e' represents the identity element of H, is called the ***kernel*** of f, denoted by $Ker(f)$.

Theorem 2.4. Let $f : G \to H$ be a homomorphism from G to H. Then $Ker(f)$ is a subgroup of G.

Proof. It is easy to see that $\mathrm{Ker}(f)$ is a subgroup of G, because for every pair of elements $a, b \in Ker(f)$, we have that $f(a) = e'$ and $f(b) = e'$, hence $f(a.b) = f(a).f(b) = e'.e' = e'$. Thus, $a.b$ belongs to $Ker(f)$. Furthermore, for any $a \in Ker(f)$, we have that $f(a) = e'$. Thus, $f(e) = f(a.a^{-1}) = f(a).f(a^{-1}) = e'$. Consequently, $e'.f(a^{-1}) = e'$. Therefore, $f(a^{-1}) = e'$, then $a^{-1} \in Ker(f)$. □

Let $f : \mathbb{Z} \to \mathbb{Z}_n$, given by $f(a) = a \pmod n$. The kernel $Ker(f)$ is formed by the integers a such that $a \equiv 0 \pmod n$. Thus, $\mathrm{Ker}(f)$ is formed by all multiples of n. Moreover, the set of multiples of n, denoted by $n\mathbb{Z}$, is a subgroup of $\mathbb{Z}$.

Definition 2.5. Let H be a subgroup of G, then H is called ***normal subgroup*** of G, if for every $h \in H$ and every $a \in G$, then $aha^{-1} \in H$.

Theorem 2.5. Let H be a subgroup of G. H is normal if and only if H is equal to its conjugates. Equivalently, H is normal if and only if H is invariant with respect to any inner automorphism in G.

Proof. If H is normal, according to the definition, we have that for $h \in H$ and $a \in G$, then $aha^{-1} \in H$. Thus, $aHa^{-1} \subset H$. To show that $H = aHa^{-1}$, for all $a \in G$, we must show that there is no pair of distinct elements $h_1, h_2 \in H$, such that $ah_1a^{-1} = ah_2a^{-1}$. But this is easy, because supposing by contradiction that there is such a pair of elements h_1 and h_2, multiplying on the right by a, we have that $ah_1 = ah_2$. Multiplying on the left by a^{-1}, we have that $h_1 = h_2$, a contradiction.

Moreover, if $H = aHa^{-1}$ for every $a \in G$, then for any $h \in H$ and for any $a \in G$, we have that $aha^{-1} \in H$, then H is normal. □

Theorem 2.6. Let H be a subgroup of G. H is normal if and only if every left coset aH is equal to the respective right coset Ha, for all $a \in G$.

Proof. If H is normal, by theorem 2.5 we have that $H = aHa^{-1}$, therefore $Ha = (aHa^{-1})a = aH$. $\square$.

Theorem 2.7. Let $f : G \to H$ be a homomorphism form G to H. Then the kernel $\mathrm{Ker}(f)$ is a normal subgroup of G. Furthermore, H is isomorphic to the quotient group $G/\mathrm{Ker}(f)$. Reciprocally, if N is a normal subgroup of G, then the map $g : G \to G/N$, defined by $g(a) = aN$, for $a \in G$, is a homomorphism from G to G/N with kernel $\mathrm{Ker}(g) = N$.

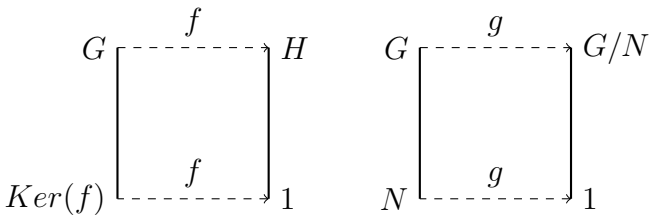

Figure 2.1: Group homomorphisms

Proof. To demonstrate that $\mathrm{Ker}(f)$ is a subgroup is trivial, because for every two elements $a, b \in \mathrm{Ker}(f)$, we have that $f(a) = f(b) = e'$, hence $f(a).f(b) = f(a.b)$. Thus, $a.b \in \mathrm{Ker}(f)$. Moreover, for every $a \in \mathrm{Ker}(f)$, we have that $f(e) = e'$, then $f(a.a^{-1}) = e'$ and then we obtain $f(a).f(a^{-1}) = e'$. Hence, $f(a^{-1}) = e'$ and thus we have that $a^{-1} \in \mathrm{Ker}(f)$. To show that it is a normal subgroup, it is enough to show that for any $a \in \mathrm{Ker}(f)$, we have that $f(a) = e'$. Therefore, for every element $g \in G$, we have to show that $gag^{-1} \in \mathrm{Ker}(f)$. But applying the function f, we have that $f(gag^{-1}) = f(g).f(a).f(g)^{-1}$. As $f(a) = e'$ and $f(g^{-1}) = f(g)^{-1}$, we have that $f(gag^{-1}) = f(g).f(g)^{-1} = e'$. Therefore, $gag^{-1} \in \mathrm{Ker}(f)$. $\square$

2.2 Rings and fields

Definition 2.6. Given a set G and two binary operations $\circ$ and $\star$, the pair $(G, (\circ, \star))$ is denominated ***ring*** if $(G, \circ)$ forms an Abelian group and $\star$ is such that the following properties are valid.

1. **Closure.** If $a \in G$ and $b \in G$, then $a \star b \in G$.
2. **Distributive law.** For any $a, b, c \in G$, then $a \star (b \circ c) = (a \star b) \circ (a \star c)$.

A ring where $a \star (b \star c) = (a \star b) \star c$, for any $a, b, c \in G$ is called ***associative ring***. A ring where there is an element $e \in G$, such that $a \star e = e \star a = a$, for any $a \in G$, is denominated ***ring with identity element***. A ring where $a \star b = b \star a$, for any $a, b \in G$, is called ***commutative ring***.

A ***field*** is a mathematical structure where the four operations are permitted, namely, $+$, $-$, $\times$ and $\div$. Let G^* be the set formed by the elements of G excluding the identity element of operation $\circ$. If $(G^*, \star)$ is an Abelian group and the distributive law, described above, is valid, then $(G, (\circ, \star))$ is a field. Given a subset $H \subset G$, if $(H, (\circ, \star))$ is a field, then H is a ***subfield*** of G. Conversely, G is called ***extension field*** of H.

Example 2.4. The set of irrational numbers $\mathbb{Q}$, together with usual addition and multiplication, forms a commutative ring, such that, for an arbitrary element $a \in \mathbb{Q}$, its additive inverse is $-a \in \mathbb{Q}$ and its multiplicative inverse is $1/a \in \mathbb{Q}$. Hence $\mathbb{Q}$ is a field. Given a ring R, we can construct an example of non-commutative ring by the utilization of square matrices of size $n \times n$, composed by elements $a_{ij} \in R$, with usual matrix addition and multiplication. The set $\mathbb{Z}_n$, with usual modular addition and modular multiplication, forms a ring, whose additive identity is 0 and multiplicative identity is 1.

Let R be a ring. A subset S of R is a ***subring*** of R if S itself is a ring with respect to the same operations defined over R.

Example 2.5. Let $\mathbb{Z}$ be the ring of integer numbers. Then, $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ is a subring of $\mathbb{Z}$, because according to example 2.2, $2\mathbb{Z}$ is an Abelian group with respect to addition. Furthermore, given two elements $a, b \in 2\mathbb{Z}$, we have that $a.b$ is even and hence belongs to $2\mathbb{Z}$. Finally, the distributive law is true because $\mathbb{Z}$ itself is a ring.

Given a ring R, a ***zero divisor*** is a non-zero element $a \in R$, such that there is $b \in R$, $b \neq 0$, such that $a.b = 0$. Let R be a commutative ring. If R contains no zero divisor the ring is called ***integral domain***. The ***characteristics*** of a ring is defined by the smallest integer n, such that

$$\sum_{1}^{n} e = 0,$$

where e is the identity element with respect to multiplication. If there is no such value n with this property, then we say that the ring has characteristics 0.

Let $\mathbb{Z}_p$ be the field from example 2.4. Thus, the smallest n such that $n.1 = 0 \pmod{p}$, is the own p. Therefore, $\mathbb{Z}_p$ has characteristics p. Let $\mathbb{Q}$ be the field defined in example 2.4. We know that there is no such value n such that $n.1 = 0$. Hence, the characteristics of $\mathbb{Q}$ is 0.

Let R be a ring with identity. R may have an element a that has no multiplicative inverse, that is, there is no a^{-1}, such that $a.a^{-1} = 1$. Otherwise, if a has an identity, it is called a ***unity*** in R. For example, in the set $\mathbb{Z}$ of integer numbers, the unities are 1 and -1. In $\mathbb{Z}_p$, for p prime, every element $a \in \mathbb{Z}_p$ has inverse a^{-1} such that $a.a^{-1} \equiv 1 \pmod{p}$ and therefore every element is a unity.

2.2.1 Ideals

Definition 2.7. Given a ring R, a subset I of R is called ***right ideal*** if I corresponds to a subgroup of R with respect to addition, and for any $x \in I$ and $r \in R$, then $xr \in I$. Given the ring R, the set I of R is denominated ***left ideal*** if I corresponds to a subgroup of R with respect to addition, and for any $x \in I$ and $r \in R$, then $rx \in I$.

If R is a commutative ring, then every right ideal is equal to the corresponding left ideal and in this case we call it an ***ideal***. A ***proper ideal*** is an ideal that is distinct from the subjacent ring. An ideal I is denominated ***prime ideal*** if for any $a, b \in R$ and $a.b \in I$, then we have that $a \in I$ or $b \in I$.

It is easy to show that $p\mathbb{Z}$ is a prime ideal, if and only if p is prime, because given $n = a.b$, n belonging to $n\mathbb{Z}$, but $a \notin n\mathbb{Z}$ and $b \notin n\mathbb{Z}$. On the other hand, given a prime p and integers a and b such that $a.b \in p\mathbb{Z}$, then $a.b = k.p$, for some integer k. Therefore, $p \mid a$ or $p \mid b$.

Let R be a commutative ring. An ideal I of R is denominated ***principal ideal*** if there is $a \in R$, such that the ideal is generated by multiplying each element from R by a. We say that the ideal is ***generated by*** a and denote it by $I = (a)$.

A function $N : R \to \mathbb{R}^+$, such that $N(0) = 0$, is called ***norm*** over an integrity domain R, if the following condition holds: (i) $N(a) > 0$ for all $a \neq 0$; (ii) $N(k.a) = |k|.N(a)$, for any integer k; and (iii) $N(a + b) \leq N(a) + N(b)$ (triagle inequality).

An ***Euclidian domain*** is an integrity domain R such that we can define a division-with-remainder algorithm, namely, given $a, b \in R$, with $b \neq 0$, we can write $a = b.q + r$, where $N(r) < N(b)$. The element r is denominated ***remainder*** and the element q is called ***quotient***. An interesting property, that is easy to demonstrate, is that every ideal I in an Euclidian domain R is a principal ideal. To show that, it is enough to consider the element d of minimum norm in I and show that the following statements are valid: (i) $(d) \subseteq I$ and (ii) $I \subseteq (d)$. The statements together allow us to conclude that $I = (d)$. The statement (i) is simple, because $d \in I$ and I is closed

with respect to multiplication. To prove statement (ii), consider any element $a \in I$. Using the division-with-remainder algorithm, we have that $a = d.q + r$. However, by minimality of d, we conclude that $r = 0$. Therefore, $a \in (d)$.

Consider from now on the commutative ring R. An ideal I of R is denominated ***maximal ideal*** if there is no ideal J of R, such that I is a proper subset of J. Moreover, R is called ***principal ideal domain*** if every ideal I of R is a principal ideal. The integers $\mathbb{Z}$ are an example of principal ideal domain, because they form an Euclidian domain.

Definition 2.8. Given a ring R and a subset $S = \{x_1, \ldots, x_k \mid x_i \in R\}$, we define the ideal I, ***generated by*** S, as being

$$\{r_1 x_1 + \cdots + r_k x_k \mid r_i \in R\}.$$

The subset S can be seen as a basis to the ideal I if $|S|$ is minimal, in other words, if there is no smaller subset that generates the same ideal.

2.2.2 Ring homomorphisms

It is possible to extend the definition of group homomorphisms to ring homomorphisms:

Definition 2.9. Given two rings R and S, where $+_R$, $+_S$, $\times_R$ and $\times_S$ are the addition and multiplication in R and S, respectively. We say that $f : R \to S$ is a ***ring homomorphism***, if and only if $f(a +_R b) = f(a) +_S f(b)$ and $f(a \times_R b) = f(a) \times_S f(b)$ holds.

The kernel of the homomorphism is also analogously defined as $\mathrm{Ker}(\psi) = \{a \in R \mid \psi(a) = 0\}$. Namely, it is the set formed by the elements $a \in R$ that are mapped to the additive identity in S.

Theorem 2.8. Let $\psi : R \to S$ be a homomorphism from R to S. Then $\mathrm{Ker}(\psi)$ is an ideal of R and S is isomorphic to the quotient ring $R/\mathrm{Ker}(\psi)$. On the other hand, if J is an ideal of R, then the map $\psi : R \to R/J$, defined by $\psi(a) = a + J$, for $a \in R$, is a homomorphism whose kernel is J.

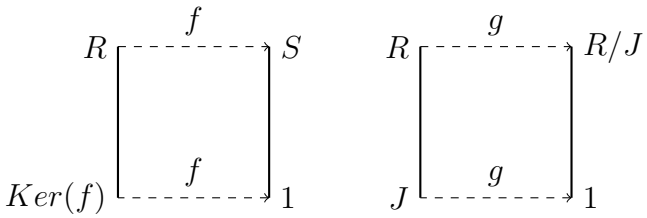

Figure 2.2: Ring homomorphisms

Theorem 2.9. Let R be a commutative ring with identity. Then

(i) an ideal I of R is maximal if and only if R/I is a field;

(ii) an ideal I of R is a prime ideal if and only if R/I is an integrity domain;

(iii) every maximal ideal is a prime ideal;

(iv) if R is a principal ideal domain, then $R/(c)$ is a field if and only if c if a prime element of R.

Definition 2.10. Ideals R_1 and R_2 in a ring R are ***comaximal*** if $R_1 + R_2 = R$.

2.2.3 Chinese remainder theorem

In this section we describe an important and old theorem, known as the ***Chinese remainder theorem*** (CRT). It has important applications in lattice-based cryptography and specially in homomorphic encryption, because it allows to encode information into ***slots*** that can be processed in parallel. The theorem was originally proposed around the third century by Sun Tsu and his famous example asks to find the smallest positive integer number x such that $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$ and $x \equiv 2 \pmod 7$. This system of modular equations can be generalized as follows:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

We have that, for every $1 \leq i \leq k$ and any $a_i \in Z_{m_i}$ this equations have an unique solution x modulo $m = \prod m_i$ if and only if $\mathrm{GCD}\,(m_i, m_j) = 1$, for all distinct $1 \leq i, j \leq k$. It is possible to calculate this solution using a constructive method, in resemblance with solving a linear system of equations, where we repeatedly isolate and substitute variables to find the solution. However, it is conceptually better here to study this theorem by considering the homomorphism $f_{\mathrm{CRT}} : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$, given by

$$f_{\mathrm{CRT}}(x) = (x \pmod{m_1}, \ldots, x \pmod{m_k}).$$

Theorem 2.10. The map f_{CRT} is a ring homomorphism. Moreover, f_{CRT} is a bijection, thus it is an isomorphism.

Proof. It is straightforward to show that f_{CRT} is an injective map, since if $f_{\mathrm{CRT}}(x) = f_{\mathrm{CRT}}(x)'$, then we have that $m_i \mid x - x'$ for all $0 \leq i \leq k$. Thus, since all m_i are relatively prime, we conclude that $m \mid x - x'$, therefore $x \equiv x' \pmod{m}$. In order to prove that f_{CRT} is surjective, it suffices to show that the range of f_{CRT} has the same cardinality as the domain, what is trivial, since the cardinality of $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ is equal to $m = \prod m_i$. □

The CRT theorem is not only valid for integers, but it appears also in many other algebraic structures, as for example polynomial rings and number fields. Thus, it is interesting to consider its abstract version, as described in next theorem.

Theorem 2.11. Let $R_1, R_2, \ldots, R_k$ be ideals in a ring R. The map $R \to R/R_1 \times R/R_2 \times \cdots \times R/R_k$, defined by $r \to (r + R_1, r + R_2, \ldots, r + R_k)$ is a ring homomorphism with kernel $R_1 \cap R_2 \cap \cdots \cap R_k$. If for any pair of distinct i, j, we have that R_i and R_j are comaximal, then the map is surjective and $R_1 \cap R_2 \cap \cdots \cap R_k = R_1 R_2 \ldots R_k$. Therefore

$$R/(R_1 R_2 \ldots R_k) \equiv R/R_1 \times R/R_2 \times \cdots \times R/R_k.$$

2.2.4 Cyclotomic rings

Let $n \in \mathbb{Z}$ (usually a power of 2) and consider the ***cyclotomic polynomial*** $\phi_n(x)$, of degree equal to $\varphi(n)$. In the case n is a power of 2, we have that the degree of ϕ_n is equal to $\varphi(n) = n/2$. Given a certain $p \in \mathbb{Z}$, we have that if $\zeta_n \in \mathbb{Z}_p$, where ζ_n is a primitive m-th root of unity in $\mathbb{Z}_p$, then $\phi_n(x)$ can be decomposed into $\ell = \phi(n)/d$ ideals by the Chinese remainder theorem (CRT), for $p^d \equiv 1 \pmod{n}$. Specifically, in the case $d = 1$, we say that the polynomial ***splits completely*** and thus we have that $\phi_n(x) = \prod_{i \in \mathbb{Z}_n^\star}(x - \zeta_n^i)$, where $\mathbb{Z}_n^\star$ is the set formed by elements in $\mathbb{Z}_n$ that are relatively prime to n.

Example 2.6. Consider the ring $R = \mathbb{Z}_5/(x^2 + 1)$. We have that $(x^2 + 1)$ is the 4-th cyclotomic polynomial and 2 is a primitive 4-th root of unity in $\mathbb{Z}_5$. Thus, we have that $(x^2 + 1) \equiv (x + 2)(x + 2^3) \equiv (x + 2)(x + 3)$.

Let $R = \mathbb{Z}[x]/\phi_n(x)$. Then we call R the ***n-th cyclotomic polynomial ring***. Let $R_p = R/pR$. A polynomial $a(x) \in R_p$ can be represented by a vector of its coefficients in $\mathbb{Z}_p$, called ***coefficients representation***. If indeed $\mathbb{Z}_p$ contains a primitive n-th root of unity ζ_n and if $p^d \equiv 1 \pmod{n}$, we can represent $a(x)$ using evaluations over the distinct primitive n-th roots of unity, given by the powers ζ_n^i, for i an integer prime with n. This representation is called the ***evaluation representation***. Although n must not be restricted to a power of 2, the case $n = 2^k$ is easier to work and have interesting properties for cryptographic usage. Namely, the evaluation representation can be computed using the ***fast Fourrier transform*** (FFT) in time $n \log n$. Afterwards, such a

representation allows us to compute ring additions and multiplications component-wisely, what means that these operations can be calculated in linear time. Moreover, it can be computed in parallel.

Given an element $a \in R$, it determines an ideal in R and the corresponding ***ideal lattice*** $\mathcal{L}_a$. Such a lattice can be used as the underlying algebraic structure for cryptographic constructions, in the sense that breaking the security of the encryption scheme can be shown to be as hard as a certain lattice problem, which is conjectured to be ***computationally hard***, as we are going to see later.

2.2.5 Canonical embedding

It is a common approach in ideal lattice cryptography to represent ideal elements using the ***canonical embedding***, as we are going to describe in this section. This representation is interesting because it offers some advantages, like for example component-wise additions and multiplications by the CRT theorem, a better analysis to the underlying ring ***expansion factor***, which is the measure of how much is the growth of elements after multiplications. Also, it has interesting automorphisms, given by the permutation of the axes of the embedding. Lyubashevsky, Peikert and Regev argue that the canonical embedding in some sense is the right way to represent elements in ideal lattice cryptography [LPR10].

Definition 2.11. A ***number field*** K is a field extension of the rationals. Precisely, it is the adjunction to $\mathbb{Q}$ of an abstract element ζ, such that $f(\zeta) = 0$ for a monic $f(x) \in \mathbb{Q}[x]$. The polynomial f is called the ***minimal polynomial*** of ζ and we say that K has degree m, where m is the degree of f.

A number field K can be interpreted as a m-dimensional vector space over $\mathbb{Q}$ with basis given by the powers ζ^i, for $0 \leq i < m$. This basis is called the ***power basis*** of K. Also, we have that the number field K is isomorphic to $\mathbb{Q}[x]/f(x)$. In particular, we have that if $f(x)$ is a cyclotomic polynomial, then ζ is a primitive m-th root of unity.

Definition 2.12. Given a number field K, the ***ring of integers*** $\mathcal{O}_K$ is formed by the algebraic integers of K, i. e. by elements whose minimal polynomial has integer coefficients.

Specifically, we are interested in the cyclotomic ring $R = \mathbb{Z}[x]/\phi_n(x)$, where we have that $m = \varphi(n)$, and the power basis $\{1, \zeta, \ldots, \zeta^{m-1}\}$ is an integral basis, thus it is also a basis to the ring of integers $\mathcal{O}_K$.

Definition 2.13. Given a degree-m number field K, we have m ring homomorphisms $\tau_i : K \to \mathbb{C}$, for $0 \leq i < m$, mapping ζ to each of the complex roots of the minimal polynomial of ζ. This family of maps gives rise to the ***canonical embedding*** of the number field K, which is defined by the map $\tau : K \to \mathbb{C}^m$, where $\tau(x) = (\tau_0(x), \tau_1(x), \ldots, \tau_{m-1}(x))$.

For cyclotomic rings R, we have that $\tau_i(\zeta) = \zeta^i$, for $i \in \mathbb{Z}_n^\star$. Hence the roots of unity $\tau_i(\zeta)$, for $0 \leq i < m$, have norm equal to 1. The expansion factor improvement is given by $\Omega(\sqrt{n})$ and a complete description of the subjacent mathematics and algorithms to do computations using the canonical embedding is presented in another work of Lyubashesky, Peikert and Regev [LPR13].

3 Probability

The study of propability theory is essencial to cryptography and in this section we are going to provide a few results that are important to understand key concepts in lattice-based cryptography, as is the case of the leftover hash lemma.

We denote by $\Pr[\text{event} \mid \text{conditions}]$ the probability that an ***event*** happens given that some ***conditions*** are satisfied. In particular we are only interested in discrete probabilities, which means that all events are sampled from a discrete set S, called ***sample space***. In general, events will be described by binary strings of fixed length,

say k, and the sample space S will be given by all possible binary strings of bit length equal to k. Then, we have that $S = \{0,1\}^k$. Any event $a \in S$ have $\Pr[a] \geq 0$. Also, the probability of all the events together sums up to 1, i. e. $\sum_{a \in S} \Pr[a] = 1$. We say that two events a and b are ***independent*** if $\Pr[a \wedge b] = \Pr[a].\Pr[b]$, where $a \wedge b$ symbol is used to denote that both events a and b happens.

A ***random variable*** X is associated to a ***probability distribution*** $\mathcal{D}$ if the probability that the random varialbe X is equal to any event $x \in S$ is determined by $\mathcal{D}$. For example, the ***uniform*** distribution is the one that gives equal probabilities to every possible event, i. e. $\Pr[X = x] = 1/|S|$.

Definition 3.1. The ***expectation*** E of a random variable X is defined by

$$E[X] = \sum_{x \in S} x.\Pr[X = x].$$

In cryptography, we usually want to show that a certain distribution is very close to the uniform distribution. Hence, in order to do that, we need to define how to measure the distance between two distributions.

Definition 3.2. Given two statistical distributions $\mathcal{A}$ and $\mathcal{B}$ over the same sample space S, we define their ***statistical distance*** as follows:

$$\frac{\sum_{x \in S} |\Pr[\mathcal{A} = x] - \Pr[\mathcal{B} = x]|}{2}.$$

3.1 Important inequalities

Theorem 3.1. Boole's inequality (union bound).

$$\Pr[\cup_{i=1}^{n} X_i] \leq \sum_{i=1}^{n} \Pr[X_i].$$

Proof. From set theory, we have that $\Pr[\mathcal{A} \vee \mathcal{B}] = \Pr[\mathcal{A}] + \Pr[\mathcal{B}] - \Pr[\mathcal{A} \wedge \mathcal{B}]$. In general, the following holds:

$$\Pr[\cup_{i=1}^{n+1} A_i] = \Pr[\cup_{i=1}^{n} A_i] + \Pr[A_{n+1}] - \Pr[\cup_{i=1}^{n} A_i \cap A_{n+1}].$$

Since the probability of the last term is a non-negative real value, and repeating the process, we obtain the desired result. □

Theorem 3.2. Markov's inequality.

$$\Pr[X \geq c] \leq \frac{E[X]}{c}.$$

Proof. By definition, we have that $E(X) = \sum_{x \in S} \Pr[X = x]x$. We break the summation into two parts to obtain $E(X) = \sum_{x<c} \Pr[X = x]x + \sum_{x \geq c} \Pr[X = x]x$. Again, using the fact that both summations are non-negative real values, we have that $E(x) \geq \sum_{x<c} \Pr[X = x]0 + \sum_{x \geq c} \Pr[X = x]v$. Therefore, we have that $E(X) \geq \Pr[X \geq v]v$, as we need. □

Definition 3.3. Given a random variable X, we define the ***variance*** of X by

$$\mathrm{Var}(X) = E((X - E(X))^2).$$

Theorem 3.3. Chebyshev's inequality.

$$\Pr[|(X - E(X))| \geq c] \leq \frac{\mathrm{Var}(X)}{c^2}.$$

Proof. Apply Markov's inequality using the definition of variance to get

$$\Pr[|(X - E(X))| \geq c] = \Pr[|(X - E(X))|^2 \geq c^2] \leq E((X - E(X))^2)/c^2,$$

as we want to prove. □

Theorem 3.4. Chernoff's inequality. For $1 \leq i \leq n$, let X_i be mutually independent random variables, such that $0 \leq X_i \leq 1$. Define $X = \sum X_i$. Then, for any $c > 1$, we have that

$$\Pr\left[T \geq cE[X]\right] \leq e^{-zE[X]},$$

for $z = c \log c + 1 - c$.

We have that Chebyshev's bound is an improvement to the result achieved by Markov, because by looking at the variance, we have a quadratic dependence on the constant c. If we add the mutual independency constraint, then we obtain a much better bound, given by Chernoff's inequality, which turns out to offer an exponential dependency on c.

3.2 Leftover hash lemma

The leftover hash lemma [HILL99] is an important tool in lattice-based cryptography. Essentially, it is used to show that a random combination of public values may have a very close statistical distance to the uniform distribution and this fact is useful to prove the security of cryptosystems.

Definition 3.4. Let $\mathcal{H} : \mathcal{D} \to \mathcal{R}$ be a family of hash functions with domain $\mathcal{D}$ and range $\mathcal{R}$. We say that $\mathcal{H}$ is a ***universal family*** of hash functions if $h \in \mathcal{H}$ is a uniformly chosen hash function, then for any $x \neq y$ and $x, y \in \mathcal{D}$ we have that

$$\Pr[h(x) = h(y)] \leq 1/|\mathcal{R}|.$$

A universal hash function is a function whose probability distribution has the property that collisions occur with at most the same probability as the uniform distribution. An stronger property is defined next.

Definition 3.5. Let $\mathcal{H} : \mathcal{D} \to \mathcal{R}$ as above. We say that $\mathcal{H}$ is a ***pairwise independent family*** of hash functions if $h \in \mathcal{H}$ is a uniformly chosen hash function, then for any $x \neq y$ and $x, y \in \mathcal{D}$ and any $r_1, r_2 \in \mathcal{R}$ we have that

$$\Pr[h(x) = r_1 \wedge h(y) = r_2] = 1/|\mathcal{R}|^2.$$

If we want to construct a cryptographic object that is indistinguishable from the uniform distribution, like for example to build functions whose output looks like a pseudorandom function, we must describe a mechanism to measure how far some distribution is from uniformity. Next we formalize the notion of closeness to the uniform distribution.

Definition 3.6. We say that a distribution is ϵ***-uniform*** if its statistical distance to the uniform distribution is bound above by ϵ.

Theorem 3.5. Leftover hash lemma. Let $\mathcal{H} : \mathcal{D} \to \mathcal{R}$ be a pairwise independent family of hash functions. If $h \in \mathcal{H}$ and $x \in \mathcal{D}$ are uniformly and independently chosen, then $h, h(x)$ are $1/2\sqrt{|\mathcal{R}|/|\mathcal{D}|}$-uniform over $\mathcal{H} \times \mathcal{R}$.

4 Lattices

In this section we give the main definitions and concepts about lattices. This area of mathematics is also known as ***geometry of numbers*** and was started by Hermann Minkowski in the end of nineteenth century. We also will present hard problem over lattices which are important for cryptography since they allow ***worst-case*** reductions, as we are going to detail later. Lattices are also important to cryptography because they are part of the ***post-quantum cryptography***, due to the fact that quantum computers can not solve, at least with asymptotic gain over classical computers, some problems over lattices that we are going to describe in this section. Such problems can be reduced to intermediary problems, such as SIS and LWE, which are the base of many cryptosystems.

Definition 4.1. Formally, lattices are defined as a linear combination of n elements $b_1, \ldots, b_n \in \mathbb{R}^n$, linearly independent, denominated ***lattice basis***.

$$\mathcal{L}(b_1, \ldots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z} \right\}.$$

In other words, a lattice is a discrete vector space, i. e. there is an analogy that allows us to use concepts like norm, dimension, orthogonality, linear transformation, etc. An alternative approach is the utilization of matrix notation, where the basis is represented by a matrix $B = [b_1, \ldots, b_n]$, that belongs to $\mathbb{R}^{n \times n}$. The lattice generated by matrix B is defined by $\mathcal{L} = \{Bx \mid x \in \mathbb{Z}^n\}$, such that the determinant $\det(B)$ is independent from basis choice and corresponds geometrically to the inverse of lattice points density in $\mathbb{Z}^n$.

Definition 4.2. Given a lattice $\mathcal{L}(B)$, the vectors that constitute the lattice basis can be interpreted as edges of a dimension-n parallelepiped. Thus, we can define $\mathcal{P}(B) = \{Bx \mid x \in [0, 1)^n\}$, denominated *fundamental domain* of B. We can define another parallelepiped such that we have a symmetric region. In order to do that, let $\mathcal{P}_{1/2}(B) = \{Bx \mid x \in (-1/2, 1/2]^n\}$, denominated *centralized fundamental domain* of B.

Theorem 4.1. Let $\mathcal{L}(B)$ be a dimension-n lattice and let $\mathcal{P}(B)$ be its fundamental domain, then given an element $w \in \mathbb{R}^n$, we can write w in the form $w = v + t$, for unique $v \in \mathcal{L}(B)$ and $t \in \mathcal{P}(B)$. This equation can be interpreted as a modular reduction, where the vector t is the result of $w \pmod{\mathcal{P}(B)}$.

The volume of the fundamental domain is given by $\mathrm{Vol}(\mathcal{P}(B)) = |\det(B)|$. Given two basis $B = \{b_1, \ldots, b_n\}$ and $B' = \{b'_1, \ldots, b'_n\}$ of the same lattice $\mathcal{L}(B)$, we have that $\det(B) = \pm \det(B')$.

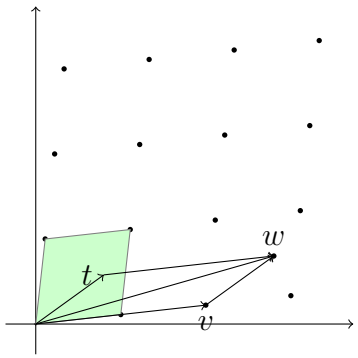

Figure 4.3: Reduction modulo $\mathcal{P}(B)$

Definition 4.3. A ***q-ary*** lattice is defined as the set $\mathcal{L}_q(A) = \{y \mid \exists s \in \mathbb{Z}^n \wedge y = As \pmod q\}$. A ***orthogonal*** lattice is the one obtained by computing a basis composed by vectors that are orthogonal to the original basis. A ***dual*** lattice is defined as the set $\mathcal{L}(A)^* = \{y \mid \langle x, y\rangle \in \mathbb{Z}, \forall x \in \mathcal{L}(A)\}$. It is easy to show that the following relations are valid for dual, orthogonal and q-ary lattices:

$$\begin{aligned}
\mathcal{L}_q^{\perp}(A) &= \{y \mid Ay = 0 \pmod q\},\\
\mathcal{L}_q^{\perp}(A) &= q\mathcal{L}_q(A)^*,\\
\mathcal{L}_q(A) &= q\mathcal{L}_q^{\perp}(A)^*.
\end{aligned}$$

In Figure 4.4 we illustrate an example of dual lattices. In black we have a lattice given by the basis vectors $(0, 3)$ and $(1, 2)$, while its dual lattice is represented in red and its basis vectors are given by $(1, 0)$ and $(-2/3, 1/3)$.

A q-ary lattice can be represented by a $q \times q$ grid, as shown in figure 4.5. Although there is just a limited amount of points inside this region, if we place many copies of it side by side we obtain a regular lattice, with the same basis, but without reduction modulo q.

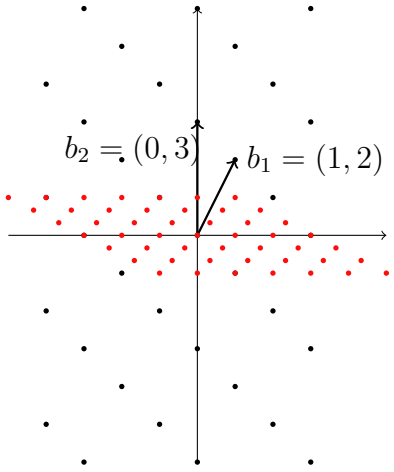

Figure 4.4: Dual lattices

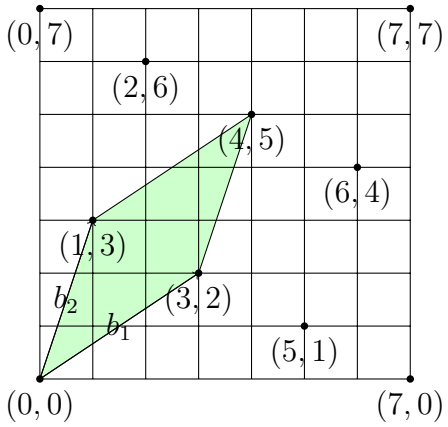

Figure 4.5: Q-ary lattice

4.1 Hard lattice problems

The problem of finding the shortest vector in a lattice, called the ***shortest vector problem*** (**SVP**) is a fundamental question in lattices. Rigorously, given a lattice $\mathcal{L}(B)$, we wish to find a non-zero vector with minimum norm. This problem can be studied considering two perspectives:

- **search problem:** find a non-zero lattice vector such that its distance from origin is minimized;
- **decision problem:** given a certain norm, determine if there is a vector or not whose length is less than or equal to that norm.

An algorithm to solve the search problem can be used to solve the corresponding decision problem. Moreover, hardness results for the decision problem implies hardness of the search problem. Hence, we can focus on decision problem and if not explicitly mentioned, notation **SVP** refers to the decision version. In practice an approximation factor $\gamma(n)$ is used, in other words we want to decide if there is a vector whose norm is inferior to a certain norm multiplied by $\gamma(n)$. Thus, lattice problems can be studied in the context of ***promise problems***, in which instances are guaranteed to belong or not to a determined subset of all possible instances. In this sense, we

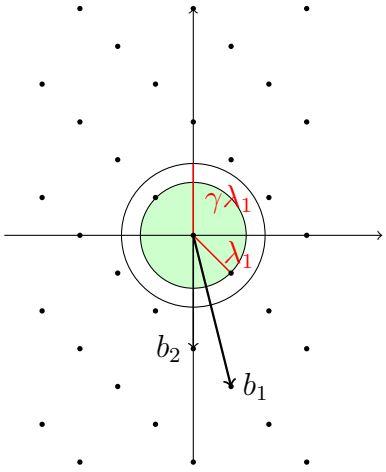

Figure 4.6: GAP**SVP**$_\gamma$ example

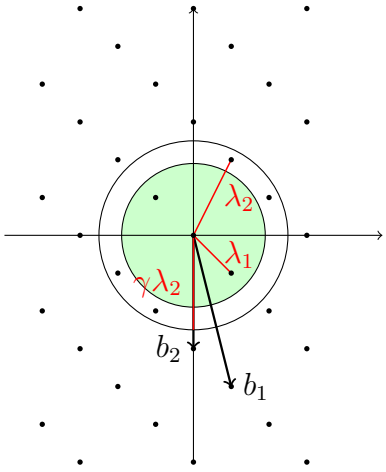

Figure 4.7: GAP**SIVP**$_\gamma$ example

denote by GAP**SVP**$_\gamma$ (where n is omitted in order to maintain a cleaner notation), this promise problem using the approximation factor $\gamma(n)$.

Ajtai proved that **SVP** is NP-hard for a random class of lattices [Ajt96]. In 1998, Micciancio [Mic98] proved that GAP**SVP**$_\gamma$ is NP-hard for an approximation factor inferior to $\sqrt{2}$, using Euclidian norm. Later, the approximation factor was improved to obtain $\gamma(n) = n^{O(1/\log\log n)}$ [Kho00]. On the other hand, for approximation factors greater than $\sqrt{n/\log n}$, there are strong evidences that GAP**SVP**$_\gamma$ is not NP-hard [AR05].

Other lattice problems are important for cryptography, as for example:

- the ***closest vector problem*** (**CVP**). Given a lattice $\mathcal{L}(B)$ and a vector $t \in \mathbb{R}^m$, the goal is to find the vector $v \in \mathcal{L}(B)$ closest to t. If we have a bound on the distance from t to the lattice, then the problem is called ***bounded distance decoding*** (**BDD**) problem, as shown in figure 4.8;
- and the ***shortest independent vector problem*** (**SIVP**). Given a basis $B \in \mathbb{R}^{n\times n}$, the problem consists in finding n linearly independent vectors $(v_1, \ldots, v_n)$, that belong to the lattice, such that the maximum norm among vectors v_i is minimum, as shown in figure 4.7.

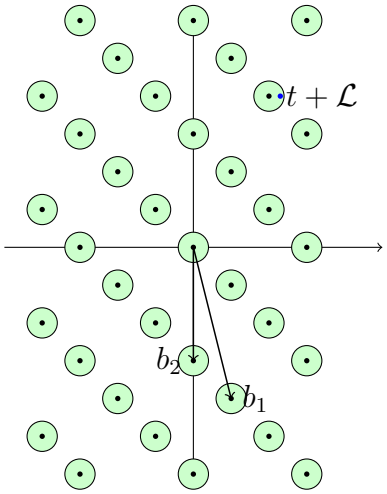

Figure 4.8: BDD example

4.2 LLL algorithm

In order to solve lattice problems, Babai proposed two algorithms [Bab86], called respectively ***rounding off*** and ***nearest plane***, that essentially proceed in the "obvious" way, but with different strategies. In the first one, it is necessary to solve a system of equations and round each obtained coordinate to the nearest integer, while the second one executes sequentially, reducing the problem in dimension n to a problem in dimension $n - 1$, further calling the algorithm recursively to obtain the desired solution. However, these algorithms achieve only approximation factor equal to c^n [MG02], for a small constant c. Nevertheless, this algorithms are important in lattice-based cryptography, because they can be used to determine concrete parameters to the cryptosystems. In general, as part of the public parameters, we have a basis to the underlying lattice, and this basis is computed using a method that turns it impossible to utilize Babai's algorithms to solve the subjacent lattice problems. The reason is that such a basis is composed by long vectors, that are not sufficiently orthogonal to each other, what makes the rounding errors grow beyond the capacity of Babai's algorithms. Hence, first of all it is necessary to run another algorithm to transform the given basis into a new basis, that makes it possible to have lower

rounding errors. Such an algorithm is called ***basis reduction***.

In 1982, in a seminal work, Lenstra, Lenstra and Lovász [LLL82] proposed a basis reduction that became famous as the ***LLL algorithm***. It can be used to solve lattice problems within exponential approximation factors $\gamma(n)$. The exact decisional shortest vector problem is known to be NP-hard, indeed if $\gamma(n)$ is less than or equal to $2^{\log n^{1-\epsilon}}$, then GAP$\mathbf{SVP}_\gamma$ is still NP-hard. For cryptographic purposes, we have that $\gamma(n)$ is given by a polynomial function and therefore the LLL algorithm can not be used to solve underlying lattice problems as indicated in Figure 4.9.

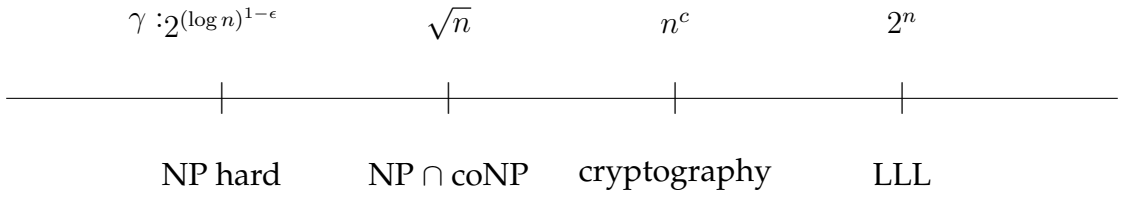

Figure 4.9: GAP$\mathbf{SVP}_\gamma$ complexity

Lagrange solved the basis reduction problem for lattices of dimension 2 [NV09]. Algorithm 4.1 shows how to compute optimal basis for such lattices. The LLL algorithm follows the same ideas of Lagrange's reduction, generalizing and relaxing them in order to obtain a polynomial time algorithm for large dimension n.

Algorithm 4.1 Gauss reduction

INPUT A basis (v_1, v_2).
OUTPUT Returns a basis with shortest vector ($v_1^\star$) and with a vector $v_2^\star$ that can not be reduced be subtracting v_1.

```
v1* = v1 and v2* = v2.
while true do
    if ||v2*|| < ||v1*|| then
        Change v1* with v2*.
    Compute m = ⌊v1*.v2*/||v1*||^2⌉.
    if m = 0 then
        return (v1*, v2*).
    Change v2* with v2* − m v1*.
```

The LLL algorithm in some sense generalizes the Euclidian algorithm to calculate

the GCD. The algorithm works based on two main steps: (i) ***size reduction***, where a vector v_i is linearly transformed into another vector that is closer to the hypherplane defined by the basis of the sublattice generated by the vectors $v_1, \ldots, v_{i-1}$; and (ii) ***Lovász condition***, that verifies if v_i is bigger than v_{i-1} multiplying by a constant $\delta = 3/4$. In special, second condition is important in order to obtain a polynomial time algorithm.

Algorithm 4.2 LLL reduction

INPUT Lattice basis $V = [v_1, \ldots, v_n]$.
OUTPUT Returns a lattice basis $V^\star = [v_1^\star, \ldots, v_n^\star]$.
  for $i = 1$ till n **do**
    for $i - 1$ till 1 **do**
      $v_i^\star = v_i^\star - c_{i,j} v_j^\star$ and $v_i^\star$ where $c_{i,j} = \lfloor \langle v_i^\star, v_j^\star \rangle / \langle v_j^\star, v_j^\star \rangle \rceil$
  if $\delta ||v_i^\star||^2 > ||\pi_i(v_{i+1}^\star)||^2$ **then**
    swap $v_i^\star$ and $v_{i+1}^\star$ and repeat.
  else
    return $V^\star$.

There are variations of the LLL algorithm described in the literature. The BKZ-β algorithm uses a subroutine to enumerate short vectors of a sublattice of small dimension β. Then, by combining with the LLL algorithm, although the enumeration considerably increases the running time, it is possible obtain a better basis. To measure the quality of the lattice reduction algorithm $\mathcal{A}$, it is useful to utilize the ***Hermite factor***, denoted by $\delta_{\mathcal{A}}$. This parameter respects the following inequality:

$$||v_1|| = \delta_{\mathcal{A}}^n \det(V)^{1/n}. \tag{1}$$

We have that the LLL algorithm achieves $\delta_{\text{LLL}} = 1.021$ and the BKZ algorithm with window size equal to 20 achieves $\delta_{\text{BKZ}-20} = 1.013$. Recently, many proposed improvements were implemented in BKZ algorithm, giving rise to the BKZ-2.0 algorithm [CN11], which can deal with window size bigger than 50 and whose Hermite factor achieves $\delta_{\text{BKZ}-2.0} = 1.007$. The Hermite factor is essencial in order to estimate the amount of operations that are necessary to break a determined cryptosystem,

thus it is a crucial value that must be considered to instantiate a concrete construction of a lattice-based cryptosystem that reaches a certain security level.

4.3 Smoothing parameter

An important concept in lattice-based cryptography is the ***smoothing parameter***. It is a very useful lattice invariant, because it allows to erase the discrete structure of a lattice, by making it hard to distinguish between a blurred lattice point and a totally random element [Pei15].

Definition 4.4. The Gaussian function $\rho_\sigma : \mathbb{R}^n \to \mathbb{R}^+$ is defined by

$$\rho_\sigma(x) = e^{\frac{-\pi||x||^2}{\sigma^2}}.$$

Given a lattice $\mathcal{L} \subseteq \mathbb{R}^n$, we define the Gaussian distribution $\mathcal{D}_{\sigma,c+\mathcal{L}}(x)$, for any coset $c+\mathcal{L}$, to be zero if x does not belong to the coset $c+\mathcal{L}$ and $\mathcal{D}_{\sigma,c+\mathcal{L}}(x) = \rho_\sigma(x)$, otherwise.

For cryptographic usage, we must be able to sample from Gaussian distributions with high precision. The following list presents the strategies that can be used to accomplish this task:

- ***rejection sampling.*** It was proposed in 2008 [GPV08a] and it works by uniformly choosing an element x in the domain of the Gaussian function and then accepting $\rho_\sigma(x)$ with proportional probability, this process is repeated while x is rejected. This strategy requires to compute exponentials by the utilization of float point arithmetic, which is computationally expensive;
- ***inversion method.*** In 2010 [Pei10], Peikert proposed using the inversion method, where we precompute the values $p_z = \Pr[x \leq z : x = \mathcal{D}_\sigma]$ and to sample the Gaussian we can simply generate a uniform element $u \in [0, 1)$ and use binary search to find z such that $u \in [p_{z-1}, p_z)$. The algorithm then outputs z.

This strategy requires large tables to store the precomputed data. In 2014, Galbraith and Dwarakanath combined this method with Knuth-Yao algorithm to obtain smaller tables. An adaptation of Ziggurat algorithm [BCG+14] is used to achieve a time-memory tradeoff. The idea is to store coordinates of rectangles of the same area, such that it is possible uniformly choose a rectangular and then use rejection sampling to sample a Gaussian inside the retangle.

A problem with this strategies is that both are not appropriate for ***constrained*** devices [DG14]. While the first one requires expensive float point arithmetic, the second one requires too large tables. A sampling algorithm for a Gaussian over the integers, similar to the Ziggurat approach, and avoiding both mentioned problems appeared in the BLISS digital signature paper [DDLL13] and, compared to many alternatives, this proposal came up to be the best choice [OPG14].

Next we give the formal definition of the smoothing parameter and some theorems.

Definition 4.5. Formally, given lattice $\mathcal{L}$ and its dual $\mathcal{L}^\star$, the smoothing parameter $\eta_\epsilon(\mathcal{L})$, for $\epsilon > 0$, is the minimal σ such that $\rho_{1/\sigma}(\mathcal{L}^\star) \leq 1 + \epsilon$.

Hence, by perturbing a lattice point using a Gaussian distribution with standard deviation bigger than the smoothing parameter we obtain cosets whose Gaussian mass are equal, except for a small error.

Theorem 4.2. [MR07] For any full rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$, we have that

$$\eta_{2^{-n}}(\mathcal{L}) \leq \sqrt{n}/\lambda_1(\mathcal{L}^\star).$$

There are related theorems in the literature [Reg05, Pei10], depending upon the underlying algebraic structure, the subjacent norm and on the specific property that we want the lattice to respect. For example, as a special case, we have Theorem 4.3

Theorem 4.3. [MR07] For any ϵ, we have that

$$\eta_\epsilon(\mathbb{Z}^n) \leq \sqrt{\log\left(2n(1+1/\epsilon)\right)/\pi}.$$

5 Lattice-based cryptography

In 1996, Ajtai proved NP-hardness of lattice problems [Ajt96], showing that a solution to average case instances could be used to find a solution in the worst case. One year later, the construction of Ajtai-Dwork cryptosystem [AD97] was proposed, playing an special role in cryptography, because it was the first construction based on ***worst case assumptions***. Other cryptographic primitives were suggested following Ajtai's work, but performance, and in special the public key size, was not good enough to be used in practice. On the other hand, GGH and NTRU are cryptosystems that have no security proof, but can be efficiently implemented [BBD08].

In this section, we are going to describe cryptographic hash constructions, encryption schemes, digital signatures and other cryptographic primitives that can be built based on assumptions over lattice problems.

5.1 Lattice-based hash

The first lattice-based cryptographic primitive to appear in the literature was proposed by Ajtai [Ajt96]. It was the appearance of ***worst case reductions***, where an attack to the cryptosystem can be used to solve any instance of hard problems over lattices. In particular, finding collisions for the proposed hash function has in average the same complexity as the SVP problem in the worst case wih respect to the subjacent dual lattice.

Concretely, given $n, m, d, q \in \mathbb{Z}$, we build a cryptographic hash family, $f_A : \{0, ..., d-1\}^m \to \mathbb{Z}_q^n$, indexed by matrix $A \in \mathbb{Z}_q^{n \times m}$. Given a vector $y \in \mathbb{Z}_d^m$, we have that $f_A(y) = Ay \pmod q$. Algorithm 5.1 describes the details invovlved in this operations. A possible parameter choice is given by $d = 2, q = n^2, m \approx 2n \log q / \log d$, such that the hash function has compression factor equal to 2.

Definition 5.1. Given the matrix $A \in \mathbb{Z}_q^{n \times m}$, the ***short integer solution*** (SIS) problem is to find short, say binary, vector x such that $Ax \equiv 0 \pmod q$.

It is possible to prove that if one can solve the SIS problem, then we can use this solution to solve any instance of problems like GAP**SVP**$_{\gamma(n)}$ and GAP**SIVP**$_{\gamma(n)}$, for a polynomial approximation factor $\gamma(n)$ [BBD08].

Note that any solution to the SIS problem can be used to generate collisions to the hash family defined above. Indeed, the scheme's security follows from the fact that if one is able to find a collision $f_A(y) = f_A(y')$, then immediately we have that it is possible to compute a short vector in the dual lattice, namely $y - y' \in \mathcal{L}_q^*(A)$.

Algorithm 5.1 Ajtai's hash

INPUT Integers $n, m, q, d \geq 1$. A matrix A chosen uniformly in $\mathbb{Z}_q^{n \times m}$. A vector $y \in \{0, ..., d-1\}^m$.
OUTPUT A vector $f(y) \in \mathbb{Z}_q^n$.
return $f(y) = Ay \pmod q$.

This proposal is really simple and can be efficiently implemented, however in practice, hash functions are designed in an ***ad-hoc*** way, without theoretical garanties provided by a security proof, what allows to obtain faster algorithms than Ajtai's construction. Moreover, if an attacker has access to sufficiently many hash values, then it is possible to recover the fundamental domain of $\mathcal{L}_q^*(A)$, allowing us to compute collisions easily.

In 2002, Micciancio used cyclic lattices to obtain more efficient hash construction. Using this idea we can define the ***ring SIS*** problem analagously to Definition 5.1, but with matrix $A \in R^{1 \times m}$, for $R = \mathbb{Z}_q[x]/(x^n - 1)$, and such that we are asked to find short x such that $Ax \equiv 0 \pmod q$.

In 2011, Stehlé and Steinfeld [SS11] proposed a collision-resistent hash function family with better performance, whose construction will be important to digital signature schemes, as we are going show in section 5.3.

5.2 Lattice-based encryption

In last section we have seen the it is possible to construct collision resistant hash functions on the assumption that the SIS problem is hard. Moreover, since we have a

worst-case reduction from lattice problems to the SIS problem, then we can consider the SIS problem as an intermediate problem under which we are going to base our cryptographic constructions. In this section, we will introduce another important problem. It is called the ***learning with errors*** (LWE) problem and it also has worst case connection to lattice problems. Hence, we are going to see that both SIS and LWE can be used in the design of lattice-based cryptosystems.

5.2.1 GGH

GGH cryptosystem [GGH97] allows us to easily understand the utilization of lattices in public key cryptography. The orthonormality of the basis is a key concept in the design of this cryptosystem, because the private key is defined as a basis B_{priv}, formed by vectors with Hadamard ratio close to 1, meaning that the vectors have good orthonormality. On the other hand, the public key B_{pub} is composed by vectors with Hadamard ratio close to 0, what means that it has not a good orthonormality.

Shorty, the cryptosystem works as follows:

- the encryption algorithm adds noise $r \in \mathbb{R}^n$ to the plaintext $m \in \mathcal{L}$, obtaining the ciphertext $c = m + r$;
- the decryption algorithm must be able to remove the inserted noise. Alternatively, it is necessary to solve an instance of CVP problem.

Figure 5.10 shows a dimension 2 lattice, with basis given by vectors v_1 and v_2, almost orthogonal. Figure 5.11 shows a different basis to the same lattice, composed by vectors whose Hadamard ratio is close to zero.

In high dimension, if basis orthonormality is close to zero, then the CVP problem becomes hard to solve using basis reduction algorithms. Thus we can define the public key as a basis B_{pub}, such that $\mathcal{H}(B_{\text{pub}})$ is close to zero. Furthermore, if we know the private key B_{priv}, then it is possible to use Babai's ***rounding-off*** algorithm [Bab86], defined below in Algorithm 5.2, to recover the plaintext.

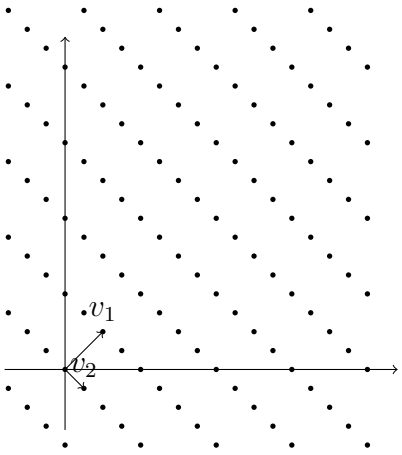

Figure 5.10: Good basis

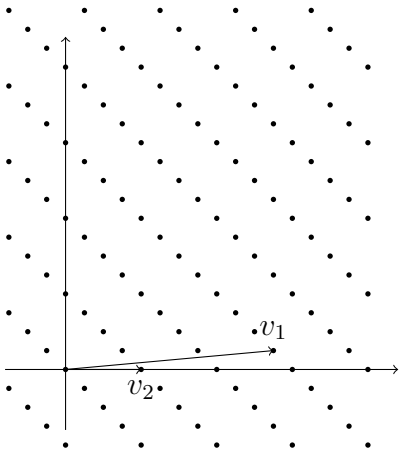

Figure 5.11: Bad basis

Algorithm 5.2 Babai's algorithm

INPUT Dimension n lattice $\mathcal{L}$; a vector $c_{B_{\text{pub}}} = (c_1, ..., c_n)$, where $c_i \in \mathbb{R}$; and a basis $B_{\text{priv}} = (s_1, ..., s_n)$, sufficiently orthonormal.

OUTPUT The vector $m \in \mathcal{L}$ that solves CVP problem with respect to c and $\mathcal{L}$.

Solve the linear system $c_{B_{\text{pub}}} = t_1 s_1 + ... + t_n s_n$, on variables t_i, for $1 \leq i \leq n$.

for $i = 0$ till $i = n$ **do**

$a_i \leftarrow \lfloor t_i \rceil$.

return $m \leftarrow a_1 s_1 + ... a_n s_n$.

The idea of Babai's algorithm is to represent the vector c using the private basis B_{priv}, solving the linear system in n equations. As $c \in \mathbb{R}^{n \times n}$, to obtain a lattice point $\mathcal{L} \subset \mathbb{Z}^n$, each coefficient $t_i \in \mathbb{R}^n$ must be approximated to the nearest integer a_i, where this operation is denoted by $a_i \leftarrow \lfloor t_i \rceil$. This procedure is simple and works very well since basis B_{priv} is sufficiently orthonormal, reducing rounding errors.

One way to attack the cryptosystem is trying to reduce the basis B_{pub}, in order to obtain shorter vector, with Hadamard ratio close to 1. In dimension 2 the problem can be easily solved using Lagrange reduction (algorithm 4.1). For higher dimensions the problem is computationally hard. Unfortunately, this scheme has no security proof and therefore we have no garantees that it is as secure as solving lattice problems.

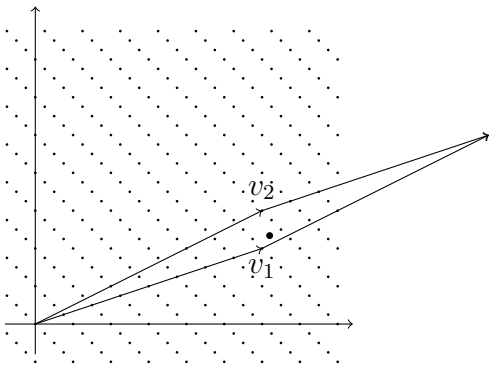

Figure 5.12: Bad basis CVP

5.2.2 The NTRU cryptosystem

NTRU cryptosystem [HPS98] is constructed over polynomial rings, but similarly to the GGH scheme we can interpret it as intances of hard problems over lattices, since key recovery and decoding attacks are indeed instances of the SVP and CVP problems, respectively. Hence, the solution to this problems would mean an attack to the cryptosystem, thus we must design our parameters in order to protect against basis reduction algorithms.

The cryptosystem utilizes the following polynomial rings: $R = \mathbb{Z}[x]/(x^n - 1)$, $R_p = \mathbb{Z}_p[x]/(x^n - 1)$ and $R_q = \mathbb{Z}_q[x]/(x^n - 1)$, where n, p, q are positive integers.

Definition 5.2. Given positive integers d_1 and d_2, we define $\mathcal{T}(d_1, d_2)$ as the class of polynomials that have d_1 coefficients equal to 1, d_2 coefficients equal to -1 and the remaining coefficients equal to zero. This polynomials are called ***ternary polynomials***.

Definition 5.3. The scheme is parameterized by the security parameter λ and the integers n, p, q, d, where n and p are prime numbers, $(p, q) = (n, q) = 1$ and $q > (6d + 1)p$.

Key generation. Choose $f \in \mathcal{T}(d+1, d)$ such that f has inverse in R_q and R_p. Choose also $g \in \mathcal{T}(d, d)$. Compute F_q as f inverse in R_q and, analogously, F_p the inverse of f in R_p. The public key is given by $h = F_q.g$.

Encryption. Given the plaintext $m \in R_p$ and the public key h, choose randomly $r \in \mathcal{T}(d, d)$ and output $c \equiv pr.h + m \pmod{q}$.

Decryption. Given the ciphertext c and the secret key f, compute $a = \lfloor f.c \rceil_q \equiv \lfloor pg.r + f.m \rceil_q$. Finally, the message can be obtained computing $m \equiv F_p.a \pmod{p}$. Output m.

5.2.3 LWE-based encryption

Like GGH, NTRU has not a security reduction to worst-case lattice hard problems. In this section, we are going to present a cryptosystem based on the LWE problem, that is an efficient proposal with security proof based on worst case GAP**SVP**$_{\gamma(n)}$ [Reg10], for a polynomial $\gamma(n)$, where n is the lattice dimension. This proof is a quantum reduction, i. e. it shows that an adversary that has advantage against the cryptosystem implies the existence of a quantum algorithm to solve hard problems over lattices. In 2009, Peikert showed a classical reduction to construct the security proof [Pei09], but under the price of using an exponencial (in the degree n) moduli q.

Definition 5.4. The ***LWE problem***, parameterized by n, N, q, σ consists in finding the vector $s \in \mathbb{Z}_q^n$, given equations $\langle s, a_i \rangle + e_i = b_i \pmod{q}$, for $1 \leq i \leq N$. The values e_i are small errors that were inserted accordingly to the distribuiton $\mathcal{D}_{n,\sigma}$, generally taken as an n-dimensional Gaussian distribution with standard deviation given by σ.

In 2010, Lyubaskevsky, Peikert and Regev utilized polynomial rings in their pro-

posal to construct the ***ring LWE*** scheme [LPR10]. By adding algebraic structure to the LWE problem, choosing variable s, a_i and e_i as elements of a determined ring, it is possible to obtain better algorithms and better overhead. Hence, we will focus on this structured version the problem, which is called ***ideal lattice cryptography***. Let $f(x) = x^n + 1$, where n is a power of 2. Given the integer q and an element $s \in R_q = \mathbb{Z}_q[x]/f(x)$, the *ring-LWE problem* over R_q, with respect to the distribution $\mathcal{D}_{n,\sigma}$, is defined correspondingly, namely, it is necessary to find s satisfying equations $a_i.s + e_i = b_i \pmod{R_q}$, for $1 \leq i \leq N$, such that a_i and b_i are elements of R_q. Modular reduction on R_q is the same as reducing by the polynomial modulo $f(x)$ and its coefficients modulo q. Also, we denote by a^T the transpose of matrix a.

Definition 5.5. The cryptosystem is parameterized by the security parameters λ and the LWE parameters n, N, q, σ. Algorithms KEYGEN, ENC, DEC are defined as follows.

Key generation. The algorithm KEYGEN(1^λ) randomly chooses the vector of polynomials $A \in R_q^N = [a_1, \ldots, a_N]^T$, where $N = n \log q$ and generates $s \in R_q$ and the vector $e \in R_q^m$ using the distribution $\mathcal{D}_{n,\sigma}$. The private key is given by $sk = s$, while the public key is given by $pk = (A, b = A.s + e)$. The output is (sk, pk).

Encryption. Given the public key pk and the message $m \in R_2$. Algorithm ENC$_{pk}(m)$ then chooses $e_1, e_2 \in R_q$, using the same distribution $\mathcal{D}_{n,\sigma}$, randomly chooses the vector of binary polynomials $r \in R_2^N$ and computes (u, v) in the following way:

$$u = A^T.r + e_1 \pmod q,$$
$$v = b^T.r + e_2 + \lfloor q/2 \rfloor.m \pmod q.$$

Decryption. Given the ciphertext (u, v) and the secret key sk, algorithm DEC computes

$$v - u.s = (r.e - s.e_1 + e_2) + \lfloor q/2 \rfloor.m \pmod q.$$

Since the standard deviation of distribution $\mathcal{D}$ is considerably less than the modulus q, we have that $(r.e - s.e_1 + e_2)$ has coefficients whose maximum length considerably less than $q/4$, and each plaintext bit can be computed using a simple computation under each coefficient of the obtained polynomial. If the coefficient is closer to 0 than $q/2$, then the corresponding bit is 0, otherwise it is 1.

Recently, a variation of the NTRU cryptosystem has been proved secure based on the assumption that the LWE problem is hard, allowing us to construct a seman-

tically secure scheme and efficient for lattice-based encryption [SS11], whose public and private keys, encryption and decryption algorithms has complexity $\tilde{O}(\lambda)$. This assymptotic complexity is remarkable because RSA, ElGamal and ECC requires for example complexity at least $\tilde{O}(\lambda^2)$. If an ideal lattice is used, the public key size is $\tilde{O}(\lambda)$, instead of quadratic in λ, hence using the ring LWE setting is important in order to make lattice-based cryptography practical, but therefore it is crucial to understand clearly the hardness of problems over this specific class of lattices. Interestingly, the SIS problem also can be stated in terms of polynomial rings, giving rise to more efficient cryptosystems [Mic07]. Till now, no attack proposed in the literature has a noticeable advantage when given an ideal lattice, that has more structure, rather than when it receives a general lattice.

The BGV homomorphic encryption scheme [GHPS12] is constructed on the assumption that the LWE problem is hard, and it turns out that the LWE problem has been a subject of interest in the cryptographic community in the last years.

5.3 Digital signatures

GGH and NTRU cryptosystems can be transformed to construct digital signature schemes [BBD08]. However, such proposals are not contemplated with a security proof and, in fact, there are attacks in the literature allowing us to recover the private key given a sufficiently big set of signatures [NR06], which permits to recover the lattice geometry by computing its fundamental domain.

In 2007, Gentry, Peikert and Vaikuntanathan [GPV08b] created a new kind of trapdoor function f, with an extra property: an efficient algorithm that, using the trapdoor, samples elements from the preimage of f. A composition of Gaussian distributions is used to obtain a point close to a lattice vector. This distribution has standard deviation greater than the basis vector within maximum norm, such that the reduction by fundamental domain has distribution that is computationally indistinguishable from the uniform distribution. Furthermore, this construction do

not reveal the lattice underlying geometry, because Gaussian distribution is spherical. Given message m and a hash function H that maps plaintexts that belong to the preimage of f, we compute the point $y = H(m)$. The signature is given by $\delta = f^{-1}(y)$. To verify the signature we compute $f(\delta) = H(m)$. This kind of construction was proposed by Bellare and Rogaway [BR93], using trapdoor permutations and modeling H as a random oracle. Thus, a digital signature scheme is constructed in the existential unforgeability under adaptative chosen plaintext attack model. We use a Gaussian to generate the noise e, such that $f(e) = y$ and $y = v + e$, for a point v chosen uniformly in the lattice. Thus, the construction has a security proof based on worst case lattice problems.

The constructions presented so far could be described in terms of two functions: $f_A(x) = Ax \pmod q$ - Ajtai's construction, based on SIS problem - and $g_A(s, e) = A^T s + e$ - Regev's construction, based on LWE problem - such that the first function is surjective and the second is injective. In 2012, Micciancio and Peikert [MP12] showed a simple, secure and efficient way to invert g_A and sample from preimage of f_A, allowing the construction of an efficient digital signature scheme. In this proposal, the Gaussian composition allowed parallelism (in later work [GPV08b], and subsequent proposals [SS11], it was inherently sequential), leading to a concrete improvement. Optimizations described above can be used in applications that are based on function g_A or sampling from preimage of f_A, hence, it is not only important to digital signature, but also to construct encryption schemes that are secure in the adaptive chosen ciphertext attack model.

Another possibility of building digital signatures based on lattice assumptions is following the Fiat-Shamir paradigm [Lyu09, Lyu12]. This kind of construction depends on the utilization of a rejection sampling algorithm, that is used to show that breaking the scheme is as hard as solving the SIS problem. In 2013, Ducas et al [DDLL13] proposed a variation based on bimodal Gaussians, called BLISS, which improves previous results, but still fails to be competitive with standard solutions such as RSA and ECDSA. For instance, we have that the public key size is equal

to 8 KBytes, while RSA has 0.5 KBytes and ECDSA has 0.02 KBytes. However, it is possible to modify the BLISS scheme to obtain better performance and smaller keys. A security analysis were carried out to obtain parameters for differente security levels, based on lattice basis reduction BKZ algorithm achieving Hermite factor $\delta = 1.007$. Indeed, a proof-of-concept was implemented and the results was encouraging. It showed that this modified BLISS is in fact competitive with RSA and ECDSA [Lep14].

6 Other applications

Lattice-based cryptography is interesting not only because it resists to quantum attacks, but also because it have been a flexible alternative to the cosntruction of cryptosystems. In particular, the ring-LWE problem has became more and more important, as it allows us to construct stronger trapdoor functions, with better parameters for both security and performance [MP12].

Gentry [Gen13] analyzed how flexible a cryptosystem can be, considering not just fully homomorphic encryption, that allows us to compute over encrypted data, but also with respect to access control. Thus, lattice-based cryptography seems to be, according to Gentry, a feasible alternative to explore the limits of cryptomania. Among other applications, it is possible to emphasize the following:

- **multilinear maps**. This is the generalization of the kind of construction that can be achieved with bilinear pairings, that is a map allowing the ***bilinear*** property in its two arguments. This property can be used in different contexts, as for example on identity based encryption. A secure multilinear map construction would be very useful and although every construction proposed till now was attacked [GGH13a], it has been object of intense research, because such a primitive would allow the design of new applications;
- **identity based encryption**. For a time, identity based encryption was only

achievable by the utilization of bilinear pairings. Using lattices, many proposals were done [BGH07, GPV08b], built upon the dual scheme $\mathcal{E}$, composed by the algorithms $\{\mathrm{DualKeyGen}, \mathrm{DualEnc}, \mathrm{DualDec}\}$, as pointed out in section 5.2.3. Specifically, $\mathrm{DualKeyGen}$ computes the private key as the error e, chosen using the Gaussian distribution, while the public key is given by $u = f_A(e)$. To encrypt a bit b, the algorithm $\mathrm{DualEnc}$ chooses randomly s, chooses x and e' according to the Gaussian and computes $c_1 = g_A(s, x)$ e $c_2 = u^T s + e' + b.\lfloor q/2 \rfloor$. The ciphertext is $\langle c_1, c_2 \rangle$. Finally, $\mathrm{DualDec}$ computes $b = c_2 - e^T c_1$. Then, given the hash function H, modeled as a random oracle, mapping identities to public keys of the dual cryptosystem, the identity based encryption scheme was constructed as follows:

- Setup. Choose the public key $A \in \mathbb{Z}_q^{n \times m}$ and the master key as been the trapdoor s, acoording to the description in section 5.3;
- Extraction. Given the identity id, we compute $u = H(\mathrm{id})$ and the decryption key $e = f^{-1}(u)$, using the trapdoor preimage sampling algorithm with trapdoor s;
- Encrypt. Given bit b, return $\langle c_1, c_2 \rangle = \mathrm{DualEnc}(u, b)$;
- Decrypt. Return $\mathrm{DualDec}(e, \langle c_1, c_2 \rangle)$.

- **functional encryption**. Functional encryption is a new primitive in cryptography, that raises new horizons [LOS+10]. In this system, a public function $f(x, y)$ determines what the user that knows the key y can infer from a ciphertext, denoted by c_x, according to parameter x. Within this model, who encrypts a message m can previously choose what kind of information is obtained after decryption. Moreover, a trusted party is responsible for key s_y generation, that can be used to decrypt c_x, returned as output for $f(x, y)$, without necessarily revealing information about m. Within this approuch it is possible to define an identity based encryption scheme as a functional encryption special case,

such that $x = (m, \mathrm{id})$ and $f(x, y) = m$ if and only if $y = \mathrm{id}$. A recent result [GGH+13b] proposes the construction of a functional encryption scheme based on lattices, being able to deal with any polynomial size Boolean circuit;

- **attributed based encryption**. This is again a special case of functional encryption, because we can define $x = (m, \phi)$ and $f(x, y) = m$ if and only if $\phi(y) = 1$. Namely, the decryption works if the decrypter's attribute y satisfies the predicate ϕ, such that the encrypter can determine a access control policy (predicate ϕ) for the cryptosystem. There are proposals to achieve this kind of operations based on LWE problem [SW12] and the multilinear maps construction mentioned above has been used by Sahai and Waters [GSW13] to propose an attributed based scheme for any Boolean circuit, showing one more time that lattice-based cryptography can be somewhat versatile;
- **obfuscation**. There is a negative result proving that obfuscation is impossible in a determined security model. However, lattices where used to construct ***indistinguishability obfuscation***, using a different security model and obtaining a good solution regarding this new model. The construction is based on the LWE problem [GGH+13b], but it is not yet efficient enough to be used in practice.

References

[AD97] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing*, STOC '97, pages 284–293, New York, NY, USA, 1997. ACM.

[Ajt96] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, STOC '96, pages 99–108, New York, NY, USA, 1996. ACM.

[AR05] D. Aharonov and O. Regev. Lattice problems in NP ∩ coNP. In *In IWPEC, volume 5018 of Lecture Notes in Computer Science*, page 765. Springer, 2005.

[Bab86] L. Babai. On Lovász lattice reduction and the nearest lattice point problem. *Combinatorica*, 6, 1986.

[BBD08] D. J. Bernstein, J. Buchmann, and E. Dahmen. *Post-Quantum Cryptography*. Springer, Heidelberg, Deutschland, 2008.

[BCG+14] J. Buchmann, D. Cabarcas, F. Göpfert, A. Hülsing, and P. Weiden. Discrete ziggurat: A time-memory trade-off for sampling from a gaussian distribution over the integers. In T. Lange, K. Lauter, and P. Lisoněk, editors, *Selected Areas in Cryptography – SAC 2013: 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers*, pages 402–417, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[BGH07] D. Boneh, C. Gentry, and M. Hamburg. Space-efficient identity based encryption without pairings. In *FOCS*, pages 647–657, 2007.

[BR93] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, CCS '93, pages 62–73, New York, NY, USA, 1993. ACM.

[CN11] Y. Chen and P. Q. Nguyen. Bkz 2.0: Better lattice security estimates. In D. H. Lee and Xiaoyun Wang, editors, *Advances in Cryptology – ASIACRYPT 2011: 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, pages 1–20, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[DDLL13] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky. Lattice signatures and bimodal gaussians. In R. Canetti and J. A. Garay, editors, *Advances in Cryptology – CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, pages 40–56, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[DF03] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2003.

[DG14] Nagarjun C. Dwarakanath and Steven D. Galbraith. Sampling from discrete gaussians for lattice-based cryptography on a constrained device. *Applicable Algebra in Engineering, Communication and Computing*, 25(3):159–180, 2014.

[Gen09] C. Gentry. Fully homomorphic encryption using ideal lattices. In *STOC '09: Proceedings of the 41st annual ACM symposium on Theory of computing*, pages 169–178, New York, NY, USA, 2009. ACM.

[Gen13] C. Gentry. Encrypted messages from the heights of cryptomania. In *TCC*, pages 120–121, 2013.

[GGH97] O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. In *Advances in Cryptology—CRYPTO '97*, Lecture Notes in Computer Science, pages 112–131. Springer-Verlag, 1997.

[GGH13a] S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices. In *EUROCRYPT*, pages 1–17, 2013.

[GGH+13b] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. *IACR Cryptology ePrint Archive*, 2013:451, 2013.

[GHPS12] C. Gentry, S. Halevi, C. Peikert, and N. P. Smart. Ring switching in BGV-style homomorphic encryption. Cryptology ePrint Archive, Report 2012/240, 2012. `http://eprint.iacr.org/`.

[GPV08a] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, pages 197–206, New York, NY, USA, 2008. ACM.

[GPV08b] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th annual ACM symposium on Theory of computing*, STOC '08, pages 197–206, New York, NY, USA, 2008. ACM.

[GSW13] C. Gentry, A. Sahai, and B. Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *CRYPTO (1)*, pages 75–92, 2013.

[HILL99] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.

[HPS98] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A ring-based public key cryptosystem. In *Lecture Notes in Computer Science*, pages 267–288. Springer-Verlag, 1998.

[Kho00] S. Khot. Inapproximability results for computational problems on lattices, 2007. survey paper preparedfor the lll+25 conference. to appear. [35. In *In Proc. 11th Annual ACM-SIAMSymposium on Discrete Algorithms*, pages 937–941. Combinatorica, 2000.

[Lep14] T. Lepoint. *Design and Implementation of Lattice-Based Cryptography*. PhD thesis, École Normale Supérieure and University of Luxembourg, June 2014.

[LLL82] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[LOS+10] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 62–91. Springer Berlin Heidelberg, 2010.

[LPR10] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. *Advances in Cryptology EUROCRYPT 2010*, 6110/2010(015848):1?23, 2010.

[LPR13] V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for ring-LWE cryptography. In *EUROCRYPT*, pages 35–54, 2013.

[Lyu09] V. Lyubashevsky. Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In M. Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009: 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-*

10, 2009. Proceedings, pages 598–616, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[Lyu12] V. Lyubashevsky. Lattice signatures without trapdoors. In D. Pointcheval and T. Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, pages 738–755, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[MG02] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: a cryptographic perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, Massachusetts, March 2002.

[Mic98] D. Micciancio. On the hardness of the shortest vector problem. Technical report, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 1998.

[Mic07] D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *computational complexity*, 16(4):365–411, 2007.

[MP12] D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 700–718. Springer Berlin Heidelberg, 2012.

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

[NR06] P. Nguyen and O. Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 271–288. Springer Berlin Heidelberg, 2006.

[NV09] P. Q. Nguyen and B. Valle. *The LLL Algorithm: Survey and Applications*. Springer Publishing Company, Incorporated, 1st edition, 2009.

[OPG14] T. Oder, T. Pöppelmann, and T. Güneysu. Beyond ecdsa and rsa: Lattice-based digital signatures on constrained devices. In *DAC*, pages 110:1–110:6. ACM, 2014.

[Pei09] C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In *Proceedings of the 41st annual ACM symposium on Theory of computing*, STOC '09, pages 333–342, New York, NY, USA, 2009. ACM.

[Pei10] C. Peikert. An efficient and parallel gaussian sampler for lattices. In T. Rabin, editor, *Advances in Cryptology – CRYPTO 2010: 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, pages 80–97, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[Pei15] C. Peikert. A decade of lattice cryptography. Cryptology ePrint Archive, Report 2015/939, 2015. `http://eprint.iacr.org/`.

[Reg05] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC '05: Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pages 84–93, New York, NY, USA, 2005. ACM.

[Reg10] O. Regev. The learning with errors problem (invited survey). In *IEEE Conference on Computational Complexity*, pages 191–204. IEEE Computer Society, 2010.

[SS11] D. Stehlé and R. Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. In *Proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology*, EUROCRYPT'11, pages 27–47, Berlin, Heidelberg, 2011. Springer-Verlag.

[SW12] A. Sahai and B. Waters. Attribute-based encryption for circuits from multilinear maps. *CoRR*, abs/1210.5287, 2012.