A brief introduction to lattices for cryptography

Léo Ducas

Lecture notes from The African Mathematical School
Bamenda, Cameroon, June 2016

1 Introduction

Cryptography Cryptography is the art of keeping communication confidential and secure. Those properties are provided by the two basic primitives: encryption and signatures. Here we are only interested in *asymmetric cryptography*: there should be two keys, a private or secret one, allowing its owner the decrypt or to sign, while the public key, which is given to everyone allows only to encrypt or to verify signatures.

Cryptography is used behind the scene each time we use our credit-card or connect to a website using the protocol `https`. Without secure cryptography, many infrastructure, including internet, would completly fall apart, making them vulnerable to attacks from hackers, totalitarian government, or rogue agencies.

To ensure that those schemes are unbreakable, cryptography relies on mathematical problems that are hard to solve. By hard, it should be understood that, given a computer, solving those problems would take millions or billions of years. More formally, cryptosystems are defined with a security parameter $\kappa > 0$, and it should be the case that the problems take exponential time 2^κ to solve given only the public key, but can be solve in polynomial time κ^c for some small constant c given the secret key.

To build such cryptosystems, one must find a mathematical structure that can be described simply, but for which some special information (the secret key) allows to do some computation that is otherwise intractable. The simplest and oldest example of such structure is an RSA modulus: the ring $\mathbb{Z}/N\mathbb{Z}$ for a composite integer $N = pq$ where p and q are primes. In that case the special knowledge is the factorization p and q. While N easily allows to encrypt a message $\mathcal{E}_N : m \to m^e \bmod N$, the knowledge of p and q allows to inverse the above function, by computing an inverse exponent d such that $ed = 1 \bmod (p-1)(q-1)$.

Motivations The RSA cryptosystem is nowadays considered quite inefficient: public-keys are large, and computations are slow. The best cryptosystems currently in use are based on elliptic curves.

Alternatives to RSA and elliptic curves have been studied, based on codes, or on lattices for example. There are many motivation to develop new cryptosystems, such as improving

efficiency, or adding new functionalities. Lattice-based-cryptography has been very successful in that regard: for example the NTRU-Encrypt scheme, based on lattices with special structures is one of the fastest scheme for that task. Another breakthrough in cryptography that came from lattices is the realization of fully-homomorphic encryption (FHE). In such an encryption scheme, one can compute "through" the encryption, that is can compute any function on ciphertexts without learning the content of the ciphertexts. This allows a lot of flexibility when using cryptography, for example when one party one to delegate computation to someone else, while keeping its data private.

Another advantage of lattice-based cryptography is that it also seems to be resistant to quantum algorithms. While the quantum computer is not working today, such computer would be able to easily break RSA and elliptic curve based cryptosystems. If it is to be realized in the next decades, we must prepare for it as soon as possible. This is another reason Lattice-based cryptography has grown very popular over the last few years.

This lecture. In most of the literature on lattice-based cryptography, an algebraic presentation is chosen, and often lattices are not even defined, and it is not always obvious to understand how those cryptosystems are connected with lattices.

While this presentation is convenient to build more and more advanced cryptosystems, the general ideas and intuitions behind those construction are not so explicit.

In this lecture we chose to instead really start from the geometric point on view on lattices, and see how those ideas naturally lead to construction of lattice-based cryptosystems. We therefore choose to be somehow formal on the definition of lattices and there properties, but will just give an overview of lattice based cryptography.

The intent is to give an intuitive geometric guide to understand recent research articles on lattice based cryptography despite their algebraic presentation. Such articles typically speaks of the Short Integer Solution problem (SIS), the Learning with Error problem (LWE), their ring variants, and the NTRU cryptosystem.

Additional resources The sources of this lecture notes, and other documents associated with those lectures are available online [1], including the slides on cryptography, and the solution in `gp` to the programming exercises.

A significant portion of those notes are adapted from the Chapter 2 of my Ph.D. thesis[2], where one may find a more complete presentation of lattices and lattice-based cryptography. It was also inspired by the lecture notes of Daniele Micciancio[3]. Both are available online (see the reference section).

For a more advanced course on lattices (with less cryptography) on can also study the lectures notes of Oded Regev[4]. For textbook on complexity theory related to lattices on can

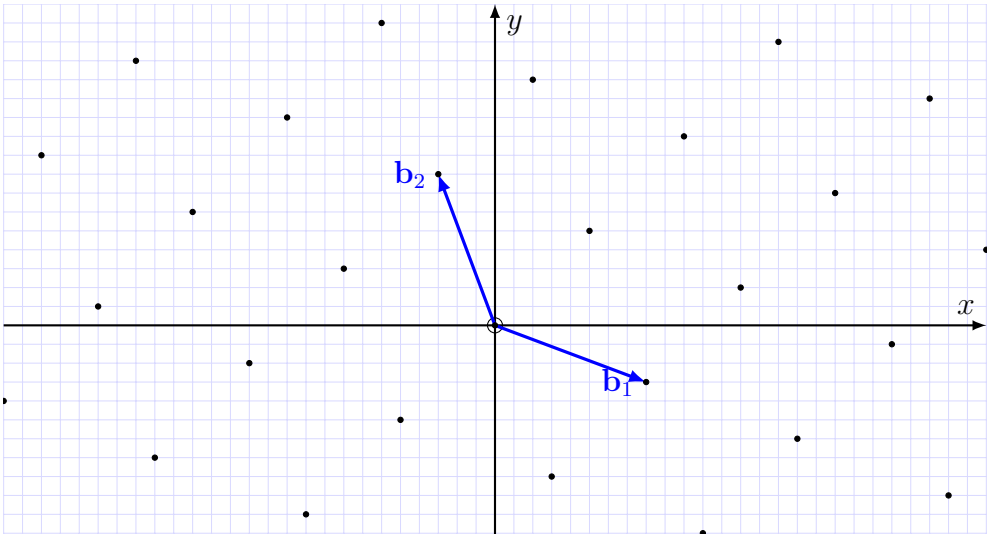
[1] `https://github.com/lducas/bamenda`

[2] `http://homepages.cwi.nl/~ducas/Thesis/index.html`

[3] `http://cseweb.ucsd.edu/classes/sp14/cse206A-a/index.html`

[4] `http://cs.nyu.edu/courses/spring13/CSCI-GA.3033-013/index.html` and `http://www.cims.nyu.edu/~regev/teaching/lattices_fall_2009/index.html`

Figure 1: A lattice in two dimension, generated by two vectors $\mathbf{b}_1, \mathbf{b}_2$.



refer to the book of Micciancio and Goldwasser. Unfortunately, no textbook on lattice based cryptography is available so far, but a long survey of Peikert[5] is also available online.

2 Lattices and basic properties

Informally, a lattice is an infinite regular grid of points in a vector space of finite dimension. Pictorially, we show a 2-dimension lattice in Figure 1.

Lattices can be defined in several ways, and it is useful to have at least the two following definitions for them. The first definition is explicit: it declares a lattice as the set of *integers* linear combinations of a *basis* $\mathbf{B}$.

Definition 1 (Lattice, explicit) *If* $\mathbf{B} = [\mathbf{b}_1 \dots \mathbf{b}_n]$ *is a matrix with linearly independent column vectors, we call lattice the set*

$$\mathcal{L}(\mathbf{B}) = \mathbf{B} \cdot \mathbb{Z}^n = \{\mathbf{Bz} : \mathbf{z} \in \mathbb{Z}^n\}$$

The second definition is implicit, and define a lattice as a discrete subgroup of the Euclidean vector space $\mathbb{R}^m$.

Definition 2 (Lattice, implicit) *A lattice* $L \subset \mathbb{R}^m$ *is a discrete subgroup of the Euclidean vector space* $\mathbb{R}^m$*; that is* L *is a non-empty subset of* $\mathbb{R}^m$ *such that:*

- *for any* $\mathbf{x}, \mathbf{y} \in L$, $\mathbf{x} - \mathbf{y} \in L$ *(*L *is a group)*

[5] `https://eprint.iacr.org/2015/939`

- $\mathbf{0}$ *is isolated in* L *that is, there exists a radius* r *such that* $r \cdot \mathfrak{B}$*, the centered* ℓ_2 *open ball of radius* r*, contains no other lattice point than* $\mathbf{0}$*:* $r \cdot \mathfrak{B} \cap L = \{\mathbf{0}\}$.

The dimension m *of the vector space containing the lattice is called the embedding dimension of the lattice* L*. The first minima* $\lambda_1(L) > 0$ *of a lattice is the largest radius* r *as above:* $\lambda_1(L) = \sup\{r \in \mathbb{R} : r \cdot \mathfrak{B} \cap L = \{\mathbf{0}\}\} = \min_{\mathbf{x} \in L \setminus \{\mathbf{0}\}} \|\mathbf{x}\|$.

While the first definition is simpler, the second definition is also very useful, as it does not require to provide an explicit basis. For example, using the second definition, it is trivial to see that the intersection $L_1 \cap L_2$ is a lattice if both L_1 and L_2 are lattices. But showing that both definition are equivalent requires a bit of effort ...

Theorem 1 (Equivalence of the two definitions) *Both definitions for lattices are equivalent, that is*

a. *If* $\mathbf{B} \in \mathbb{R}^{m \times n}$ *is a matrix with linearly independant column, show that* $\mathcal{L}(\mathbf{B})$ *is a discrete subgroup of* $\mathbb{R}^m$

b. *If* L *is a discrete subgroup of* $\mathbb{R}^m$*, then there exists a basis* $\mathbf{B}^{m \times n}$ *such that* $\mathcal{L}(\mathbf{B}) = L$.

Problem 1 *Prove the above theorem, with the help of the definitions and propositions developed below.*

Lattice are therefore discrete analogues of vector spaces. Both structures share some properties: for example, they both have bases. As vector spaces, lattices can have *many different basis*. In fact, for vector-spaces, two basis define the same vector space if and only if there is an invertible matrix sending one to the other. The situation is similar with lattices, but the transition matrices are exactly the unimodular matrices.

Proposition 2 (Relation between basis) *For any lattice* $L \subset \mathbb{R}^m$ *of dimension* n*, if* $\mathbf{B}$ *and* $\mathbf{B}'$ *are both basis of* L*, there exists an integer matrix* $\mathbf{U} \in \mathbb{Z}^{n \times n}$ *such that* $\mathbf{B} = \mathbf{B}'\mathbf{U}$ *and* $\det(\mathbf{U}) = \pm 1$.

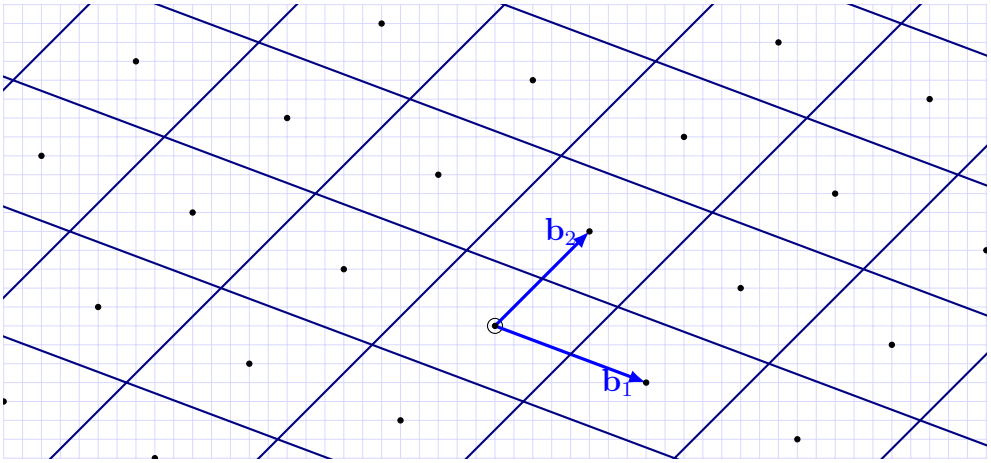
Proof: Let $\mathbf{B}$ and $\mathbf{B}'$ be bases of L. In particular, any vector $\mathbf{b} \in \mathbf{B}$ belongs to L, therefore, it can be written as a linear combination of vectors of $\mathbf{B}'$: there exists an integer matrix $\mathbf{U} \in \mathbb{Z}^{n \times n}$ such that $\mathbf{B} = \mathbf{B}'\mathbf{U}$. Similarly, there exists $\mathbf{U}' \in \mathbb{Z}^{n \times n}$ *s.t.* $\mathbf{B}' = \mathbf{B}\mathbf{U}'$. We obtain $\mathbf{B} = \mathbf{B}\mathbf{U}\mathbf{U}'$, which implies $\mathbf{U}\mathbf{U}' = \mathbf{I}_n$ because $\mathbf{B}$ has linearly independent vectors. We conclude that $\det(\mathbf{U}) \cdot \det(\mathbf{U}') = 1$; which implies $\det(\mathbf{U}) = \det(\mathbf{U}') = \pm 1$ since $\det(\mathbf{U})$ and $\det(\mathbf{U}')$ are integers. □

As for vector spaces, one can define the dimension of a lattice.

Definition 3 (Dimension of a Lattice) *The dimension of a lattice* $L \subset \mathbb{R}^m$ *is the dimension* $n \leq m$ *of the vector space it spans:* $\mathrm{Span}_{\mathbb{R}}(L)$*. Alternatively, if the lattice* L *admits a basis* $\mathbf{B} \in \mathbb{R}^{m \times n}$ *then the dimension of* $L = \mathcal{L}(\mathbf{B})$ *is* n.

If the dimension n *of* L *equals the embedding dimension* m*, then we say that the lattice* L *is full-rank.*

Figure 2: Tiling of the space with $\mathcal{P}(\mathbf{B})$



Finally, analog to sub-vector spaces also exist:

Definition 4 (Sub-lattice) *If $L, L' \subset \mathbb{R}^m$ are both lattices, we say that L' is a sublattice of L if $L' \subset L$. If L is n-dimensional, then L' is n'-dimensional for some $n' \leq n$, and $\lambda_1(L') \geq \lambda_1(L)$.*

3 Fundamental domains and volume

Given a basis of a lattice, an interesting geometrical object is the fundamental parallelepiped

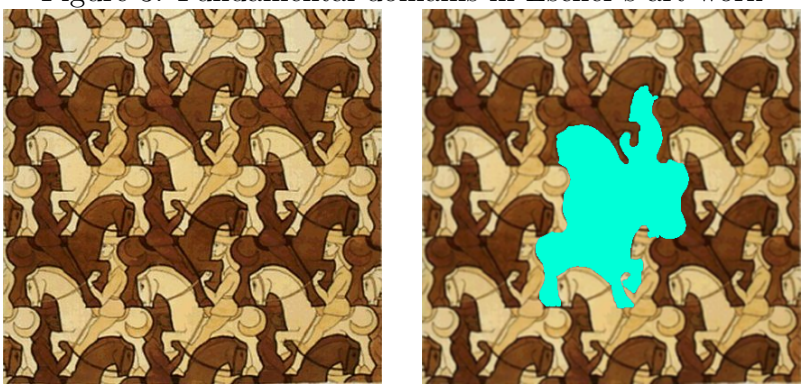
$$\mathcal{P}(\mathbf{B}) = \{\sum_{i=1}^{n} w_i \mathbf{b}_i : w_i \in [-1/2, 1/2)\}$$

associated with that basis. The following property can be interpreted geometrically as follows: if $\mathbf{B}$ is a basis of a lattice L, then the parallelepiped $\mathcal{P}(\mathbf{B})$ tiles the space with respect to L, that is, the sets $\mathbf{x} + \mathcal{P}(\mathbf{B})$ for $\mathbf{x} \in L$ covers the whole vector space $\mathrm{Span}_{\mathbb{R}}(L)$, and those shifted sets do not overlaps. This is depicted in Figure 2.

Proposition 3 *If $\mathbf{B}$ is a basis of a lattice $L = \mathcal{L}(\mathbf{B}) \subset \mathbb{R}^m$, then any $\mathbf{x} \in \mathrm{Span}_{\mathbb{R}}(L)$ can be written uniquely as $\mathbf{x} = \mathbf{v} + \mathbf{w}$ with $\mathbf{v} \in L$ and $\mathbf{w} \in \mathcal{P}(\mathbf{B})$ where $\mathcal{P}(\mathbf{B})$ denotes the parallelepiped spanned by $\mathbf{B}$: $\mathcal{P}(\mathbf{B}) = \{\sum_{i=1}^{n} w_i \mathbf{b}_i : w_i \in [-1/2, 1/2)\}$. We denote $\mathbf{x} \bmod \mathbf{B}$ the unique $\mathbf{w}$ as above.*

Proof: One can uniquely write $\mathbf{x} = \sum x_i \mathbf{b}_i$ for $x_i \in \mathbb{R}$ since $\mathbf{B}$ is a $\mathbb{R}$-basis of the vector space $\mathrm{Span}_{\mathbb{R}}(L)$. For the existence, simply choose $\mathbf{v} = \sum \lfloor x_i \rceil \mathbf{b}_i$ and $\mathbf{w} = \sum (x_i - \lfloor x_i \rceil) \mathbf{b}_i$. For uniqueness, decompose $\mathbf{v} = \sum v_i \mathbf{b}_i$ where $v_i \in \mathbb{R}$ and $\mathbf{w} = \sum w_i \mathbf{b}_i$ for $w_i \in [-1/2, 1/2)$.

Figure 3: Fundamental domains in Escher's art work



Since the vectors of $\mathbf{B}$ are linearly independent, $\mathbf{x} = \mathbf{v} + \mathbf{w}$ implies $x_i = v_i + w_i$ for all indexes i; the only decomposition of x_i as a sum of an integer and a real in $[-1/2, 1/2)$ is indeed $v_i = \lfloor x_i \rceil$ and $w_i = x_i - \lfloor x_i \rceil$. □

One note that for two bases $\mathbf{B}, \mathbf{B}'$ of the same lattice, the volume $\mathrm{Vol}(\mathcal{P}(\mathbf{B})) = \sqrt{\det(\mathbf{B}^t\mathbf{B})}$ of $\mathcal{P}(\mathbf{B})$ is equal to the volume of $\mathcal{P}(\mathbf{B}')$, simply because $\mathbf{B}' = \mathbf{B}\mathbf{U}$ for some matrix $\mathbf{U}$ of determinant ± 1:

$$\mathrm{Vol}(\mathcal{P}(\mathbf{B}')) = \sqrt{\det(\mathbf{B}'^t\mathbf{B}')} = \sqrt{\det(\mathbf{U}^t\mathbf{B}^t\mathbf{B}\mathbf{U})} = \sqrt{\det(\mathbf{U}^t)\det(\mathbf{B}^t\mathbf{B})\det(\mathbf{U})} = \mathrm{Vol}(\mathcal{P}(\mathbf{B})).$$

This allows to define the volume of the lattice independently of the choice of the basis:

Definition 5 (Volume of a lattice) *The volume of a lattice L is defined as* $\mathrm{Vol}(L) = \mathrm{Vol}(\mathcal{P}(\mathbf{B}))$ *where* $\mathbf{B}$ *is any basis of* L *($L = \mathcal{L}(\mathbf{B})$).*

Proposition 3 can be restated using the notion of fundamental domain, saying that if $\mathbf{B}$ is a basis of L, then $\mathcal{P}(\mathbf{B})$ is a fundamental domain of L. Informally, a fundamental domain of a lattice L, is a set that tiles whole vector space $\mathrm{Span}_{\mathbb{R}}(L)$. A more complicated fundamental domains is depicted on Figure 3.

Definition 6 (Fundamental Domain) *For a lattice L, a set $\mathcal{F} \subset \mathrm{Span}_{\mathbb{R}}(L)$ is called a fundamental domain of L if for all $\mathbf{x} \in \mathrm{Span}_{\mathbb{R}}(L)$ there exist a unique decomposition $\mathbf{x} = \mathbf{v}+\mathbf{f}$ where $\mathbf{v} \in L$ and where $\mathbf{f} \in \mathcal{F}$. Alternatively, $\mathcal{F}$ is a fundamental domain if the union $\bigcup_{\mathbf{v}\in L} \mathcal{F} + \mathbf{v}$ is a disjoint union, and if this union is equal to $\mathrm{Span}_{\mathbb{R}}(L)$.*

4 Gram-Schmidt orthogonalization

Before going on, please let us introduce two new notations. If V is a sub-vector space of $\mathbb{R}^m$, then $\pi_V : \mathbb{R}^m \to V$ denotes the orthogonal projection onto V. Also, for a matrix $\mathbf{B} = [\mathbf{b}_1 \dots \mathbf{b}_n]$ we will denote $\mathbf{B}_{[k]} = [\mathbf{b}_1 \dots \mathbf{b}_k]$ the partial matrix from column 1 to k.

The Gram-Schmidt orthogonalization (GSO) is an algorithm that transforms any basis $\mathbf{B}$ of a vector space to an orthogonal basis $\mathbf{B}^\star$ of the same vector space. Yet, if $\mathbf{B}$ is a basis of a lattice L, $\mathbf{B}^\star$ is not necessarily a basis of the same lattice since, all the $\mathbf{b}_i^\star$'s may not belong to L for any index $i > 1$; in general, and unlike vector spaces, lattices do not admit orthogonal base. Yet the Gram-Schmidt of a lattice basis remain a useful object. In particular, when it will come to using basis a to find close vector, the GSO can provide a better solution.

Definition 7 (Gram-Schmidt Orthogonalization (GSO)) *Let $\mathbf{B} = [\mathbf{b}_1 \dots \mathbf{b}_n] \in \mathbb{R}^{m \times n}$ be a matrix. The Gram-Schmidt Orthogonalization (GSO) $\mathbf{B}^\star = [\mathbf{b}_1^\star \dots \mathbf{b}_n^\star] \in \mathbb{R}^{m \times n}$ is defined as follows:*

$$\begin{aligned}\mathbf{b}_1^\star &= \mathbf{b}_1 \\ \mathbf{b}_i^\star &= \mathbf{b}_i - \pi_{\mathrm{Span}_{\mathbb{R}}(\{\mathbf{b}_1 \dots \mathbf{b}_{i-1}\})}(\mathbf{b}_i) \\ &= \pi_{\{\mathbf{b}_1 \dots \mathbf{b}_{i-1}\}^\perp}(\mathbf{b}_i)\end{aligned}$$

Note that this recursive definition implies that for any $k \leq n$, $[\mathbf{b}_1^\star \dots \mathbf{b}_k^\star]$ is the GSO of $[\mathbf{b}_1 \dots \mathbf{b}_k]$, in other words $(\mathbf{B}_{[k]})^\star = (\mathbf{B}^\star)_{[k]} = \mathbf{B}^\star_{[k]}$.

From this definition, we can deduce an algorithm to compute the Gram-Schmidt orthogonalization.

Algorithm 1 Gram-Schmidt algorithm

Input: A basis $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]$ of a full-rank lattice $L \subset \mathbb{R}^m$.
Output: The GSO $\mathbf{B}^\star$ of $\mathbf{B}$

1: **for** $i = 1$ to n **do**
2: $\quad \mathbf{b}_i^\star \leftarrow \mathbf{b}_i$
3: $\quad$ **for** $j = 1$ to $i - 1$ **do**
4: $\quad\quad \mathbf{b}_i^\star \leftarrow \mathbf{b}_i^\star - \frac{\langle \mathbf{b}_i^\star, \mathbf{b}_j^\star \rangle}{\|\mathbf{b}_j^\star\|^2} \cdot \mathbf{b}_j^\star$
5: return $\mathbf{B}^\star = [\mathbf{b}_1^\star, \dots, \mathbf{b}_n^\star]$

We easily see that this algorithm performs $O(n^3)$ operations on real numbers (yet it's bit-complexity may be larger if one requires the result with high precision).

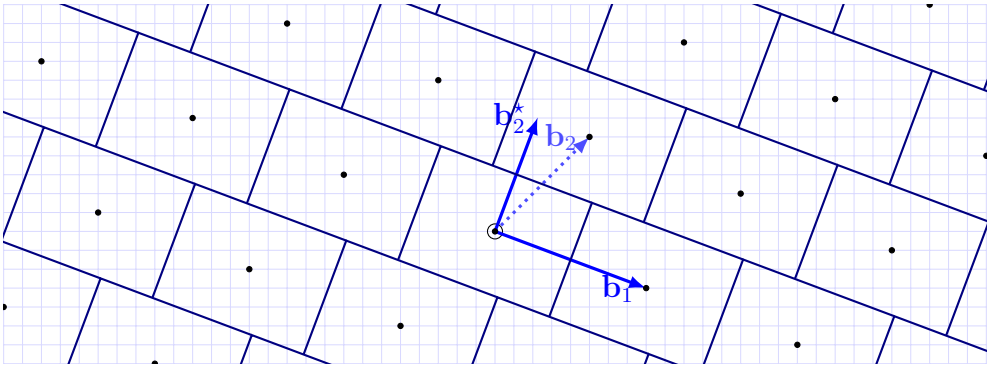
Proposition 4 (Gram-Schmidt Orthogonalization) *For any $n \times m$ real matrix $\mathbf{B}$, there exists a unique decomposition $\mathbf{B} = \mathbf{B}^\star \cdot \mu$, where $\mu = (\mu_{i,j})$ is an $n \times n$ upper-triangular matrix with unit diagonal, $\mathbf{B}^\star$ is an $n \times m$ matrix with orthogonal column vectors. The transition matrix μ satisfies*

$$\mu_{j,i} = \langle \mathbf{b}_i \, , \mathbf{b}_j^\star \rangle / \|\mathbf{b}_j^\star\|^2$$

.

In particular, this gives a relation between the GSO of a basis and the volume of a lattice its spans, namely

Figure 4: Tiling of the space with $\mathcal{P}(\mathbf{B}^\star)$



Corollary 5 *If* $\mathbf{B}$ *is the basis of a* n*-dimensional lattice* $L \subset \mathbb{R}^m$*, and* $\mathbf{B}^\star$ *is its GSO, then*

$$\mathrm{Vol}(L) = \prod_{i=1}^{n} \|\mathbf{b}_i^\star\|$$

.

Proof: Simply note that $\mathrm{Vol}(L) = \mathrm{Vol}(\mathcal{P}(\mathbf{B}))$ where

$$\mathrm{Vol}(\mathcal{P}(\mathbf{B}))^2 = \det((\mathbf{B}^\star\mu)^t(\mathbf{B}^\star\mu)) = \det(\mu^t)\det((\mathbf{B}^\star)^t\mathbf{B}^\star)\det(\mu) = \mathrm{Vol}(\mathcal{P}(\mathbf{B}^\star))^2$$

and that $\mathrm{Vol}(\mathcal{P}(\mathbf{B}^\star)) = \prod_{i=1}^{n} \|\mathbf{b}_i^\star\|$ because the $\mathbf{b}_i^\star$'s are orthogonal. □

An interesting property of the GSO $\mathbf{B}^\star$, is that, even if it *is not a basis* of the lattice $\mathcal{L}(\mathbf{B})$, the parallelepiped it spans is still a fundamental domain of $\mathcal{L}(\mathbf{B})$, as shown in figure 4.

Proposition 6 *If* $\mathbf{B}$ *is a basis of an* n*-dimensional lattice* $L = \mathcal{L}(\mathbf{B}) \subset \mathbb{R}^m$ *and if* $\mathbf{B}^\star = \mathbf{B}\mu^{-1}$ *is the GSO of* $\mathbf{B}$*, then* $\mathcal{P}(\mathbf{B}^\star)$ *is a fundamental domain.*

The proof is interesting because we can deduce an algorithm from it, called the nearest plane algorithm, that we will see later.

Proof: We proceed by induction. Recall from the definition of GSO that $(\mathbf{B}_{[k]})^\star = (\mathbf{B}^\star)_{[k]}$. For a one dimensional lattice $\mathbf{B} = [\mathbf{b}]$, we have $\mathbf{B}^\star = \mathbf{B}$, so $\mathcal{P}(\mathbf{B}^\star) = \mathcal{P}(\mathbf{B})$ is a fundamental domain of $\mathcal{L}(\mathbf{B})$.

Now, consider an n-dimensional lattice $\mathcal{L}(\mathbf{B})$. By induction, $\mathcal{P}(\mathbf{B}^\star_{[n-1]})$ is a fundamental domain of $\mathcal{L}(\mathbf{B}_{[n-1]})$. Let $\mathbf{x}$ be an arbitrary vector in $\mathrm{Span}_{\mathbb{R}}(L)$, it can be written as $\mathbf{x}' + x_n\mathbf{b}_n^\star$ where $\mathbf{x} \in \mathrm{Span}_{\mathbb{R}}(\mathbf{B}_{[n-1]})$ and $x_n \in \mathbb{R}$. Set $x_n' = \lfloor x_n \rceil \in \mathbb{Z}$, and rewrite

$$\mathbf{x} = \underbrace{\mathbf{x}' + (x_n - x_n')(\mathbf{b}_n - \mathbf{b}_n^\star)}_{\mathbf{v} \in \mathrm{Span}_{\mathbb{R}}(\mathbf{B}_{[k-1]})} + \underbrace{x_n'\mathbf{b}_n}_{\in\mathcal{L}(\mathbf{b}_n)} + \underbrace{(x_n - x_n')\mathbf{b}_n^\star}_{\in\mathcal{P}(\mathbf{b}_n^\star)}.$$

Note that $\mathbf{v} = \mathbf{x}' + (x_n - x'_n)(\mathbf{b}_n - \mathbf{b}^\star_n)$ belongs to $\mathrm{Span}_{\mathbb{R}}(\mathbf{B}_{[k-1]})$, therefore, by induction it can be written as $\mathbf{v} = \mathbf{y} + \mathbf{z}$ where $\mathbf{y} \in \mathcal{L}(\mathbf{B})$ and $\mathbf{z} \in \mathcal{P}(\mathbf{B}^\star_{[n-1]})$. We conclude on existence by checking that $\mathbf{x} = (\mathbf{v} + x'_n\mathbf{b}_n) + (\mathbf{z} + (x_n - x'_n)\mathbf{b}^\star_n)$, and that $(\mathbf{v} + x'_n\mathbf{b}_n) \in \mathcal{L}(\mathbf{B})$ and $(\mathbf{z} + (x_n - x'_n)\mathbf{b}^\star_n) \in \mathcal{P}(\mathbf{B}^\star)$.

For uniqueness, consider two decompositions of $\mathbf{x} = \mathbf{B}\mathbf{y} + \mathbf{B}^\star\mathbf{z} = \mathbf{B}\mathbf{y}' + \mathbf{B}^\star\mathbf{z}'$ where $\mathbf{y}, \mathbf{y}' \in \mathbb{Z}^n$ and $\mathbf{z}, \mathbf{z} \in [-1/2, 1/2)^n$. To prove uniqueness, we should show that $\mathbf{y} = \mathbf{y}'$ and $\mathbf{z} = \mathbf{z}'$. Consider the quantity $\langle \mathbf{x}, \mathbf{b}^\star_n \rangle$, because $\mathbf{b}^\star_n$ is orthogonal to all $\mathbf{b}^\star_i$ and $\mathbf{b}^\star_i$, we have:

$$\langle \mathbf{x}, \mathbf{b}^\star_n \rangle = y_n \langle \mathbf{b}_n, \mathbf{b}^\star_n \rangle + z_n \langle \mathbf{b}^\star_n, \mathbf{b}^\star_n \rangle = y'_n \langle \mathbf{b}_n, \mathbf{b}^\star_n \rangle + z'_n \langle \mathbf{b}^\star_n, \mathbf{b}^\star_n \rangle.$$

It remains to note that $\langle \mathbf{b}_n, \mathbf{b}^\star_n \rangle = \langle \mathbf{b}^\star_n, \mathbf{b}^\star_n \rangle = \|\mathbf{b}^\star_n\|^2$, to deduce $y_n = y'_n$ and $z_n = z'_n$. To conclude, it remains to apply the induction hypothesis on $\mathbf{x} - (y_n\mathbf{b}_n + z_n\mathbf{b}^\star_n)$ which belongs to $\mathcal{L}(\mathbf{B}_{[n-1]})$. □

5 Finding close vectors

An interesting algorithmic problem related to a lattice is the close vector problem: given a basis of a lattice $L \subset \mathbb{R}^m$, and a target point $\mathbf{t} \in \mathbb{R}^m$, find a vector $\mathbf{v} \in L$ such that $\mathbf{v}$ is close to $\mathbf{t}$.

This problem has many variant, for example the hardest variant is the closest vector problem, and this variant is known to be NP-hard, and it relates to a geometrical object called the "Voronoi cell".

The variants that we will use for cryptography are described below. Those variants are not known to be NP-hard, but are still quite hard to solve, and typically require exponential time to solve (unless one is equipped with a *good basis* of L, as we shall see below).

This first version asks one to find a solution at distance at most d, and it is implicitly assumed that d is large enough so that at least one solution exists for any target vector $\mathbf{t}$. For a more formal understanding of this implicit condition, please refer to the notion of *covering radius* of a lattice, as defined in Lecture X of XXX. One note that the larger η is, the easier the problem gets, and gets trivial for $\eta = \infty$.

Definition 8 (Close vector problem: δ-CVP) *Given the basis $\mathbf{B} \in \mathbb{R}^{n \times n}$ of a (full-rank) lattice $L \in \mathbb{R}^n$, and a target $\mathbf{t} \in \mathbb{R}^n$ find $\mathbf{v} \in L$ such $\|\mathbf{t} - \mathbf{v}\| \leq \delta$.*

A second version of this problem useful for cryptography, especially encryption is the Bounded-Distance Decoding problem (BDD). In this version, one is asked to find a very close lattice point, at distance at most $d \leq \lambda_1(L)/2$. Such condition ensures that at *most one solution* exists, and for most targets $\mathbf{t} \in \mathbb{R}^m$ there will be no such solutions. The BDD problem is therefore a problem with a promise that $\mathbf{t}$ is unusually close to the lattice L. This version is better understood as a decoding task, that is, given a noised version $\mathbf{v} + \mathbf{e}$ ($\mathbf{e}$ is a small error) of a vector $\mathbf{v} \in L$ one must remove the noise $\mathbf{e}$ to recover the "message" $\mathbf{v}$. This problem is somehow a dual problem to δ-CVP. In particular, this problem become easier when δ decreases, and gets trivial when $\delta = 0$.

Definition 9 (Bounded Distance Decoding Problem: η-BDD) *Given the basis $\mathbf{B} \in \mathbb{R}^{n\times n}$ of a (full-rank) lattice $L \in \mathbb{R}^n$, and a target $\mathbf{t} = \mathbf{v} + \mathbf{e}$ for some $\mathbf{v} \in L$ and some small $\mathbf{e} \in \mathbb{R}^n$, $\|\mathbf{e}\| \leq \eta < \lambda_1(L)/2$, recover $\mathbf{v}$ (or equivalently $\mathbf{e}$).*

As mentioned before, those problems can be solved with basis of sufficient quality. For example there is a very simple algorithm (called the round'off algorithm) that, given a target $\mathbf{t}$ finds a solution $\mathbf{v}$ such that $\mathbf{t} - \mathbf{v} \in \mathcal{P}(\mathbf{B})$. We say that this algorithm is associated with the fundamental domain $\mathcal{P}(\mathbf{B})$.

Algorithm 2 Round'off algorithm

Input: A basis $\mathbf{B}$ of a full-rank lattice $L \subset \mathbb{R}^n$, a target point $\mathbf{t} \in \mathbb{R}^n$.
Output: A decomposition $\mathbf{t} = \mathbf{v} + \mathbf{f}$ where $\mathbf{v} \in L$ and $\mathbf{w} \in \mathcal{P}(\mathbf{B})$

1: $\mathbf{x} \leftarrow \mathbf{B}^{-1}\mathbf{t}$
2: $\mathbf{y} \leftarrow (\lfloor x_1 \rceil, \ldots, \lfloor x_n \rceil)$
3: $\mathbf{v} \leftarrow \mathbf{B}\mathbf{y}$
4: $\mathbf{f} = \mathbf{t} - \mathbf{v}$
5: return $(\mathbf{v}, \mathbf{f})$

What is the "quality of the output", i.e. how large is $\mathbf{f} = \mathbf{t} - \mathbf{v}$ is ? Well, we know that $\mathbf{f} \in \mathcal{P}(\mathbf{B})$, that is $\mathbf{f} = \sum \mathbf{b}_i r_i$ for some $r_i \in [-1/2, 1/2)$. By the triangle inequality we deduce

$$\|\mathbf{f}\| \leq \frac{1}{2} \sum \|\mathbf{b}_i\|.$$

We see that the quality of the output highly depends on the "quality of the basis". The conclusion is that if we have a good basis, that is a basis such that $2\sum \|\mathbf{b}_i\| \leq \delta$, then we can solve δ-CVP quite efficiently: the above algorithm only requires $O(n^2)$ operations. But finding a good basis is also a hard problem: one must have a very special knowledge about the lattice L to solve those δ-CVP problems.

The above algorithm was rather simple, and has rather poor quality. It is possible to improve the quality a bit by using the Gram-Schmidt orthogonalization. This time we will obtain a solution $\mathbf{v}$ such that $\mathbf{t}-\mathbf{v} \in \mathcal{P}(\mathbf{B}^\star)$: this new algorithm (the nearest plane algorithm) is associated with the fundamental domain $\mathcal{P}(\mathbf{B}^\star)$. As mentionned earlier, this algorithm can be viewed as an algorithmic version of (the existence part of) the proof of Proposition 6, saying that $\mathcal{P}(\mathbf{B}^\star)$ is indeed a fundamental domain.

This algorithm also runs in time $O(n^2)$ but can solve δ-CVP for a potentially smaller δ. Another advantage is that it is also easier to find a sufficient condition for this algorithm to solve η-BDD.

Proposition 7 *The Nearest Plane Algorithm with basis $\mathbf{B}$ solves:*

- *δ-CVP for any $\delta \geq \frac{1}{2}\sqrt{\sum \|\mathbf{b}_i^\star\|^2}$*
- *η-BDD for any $\eta \leq \frac{1}{2}\min \|\mathbf{b}_i^\star\|$.*

Algorithm 3 Nearest Plane Algorithm

Input: A basis $\mathbf{B}$ of a full-rank lattice $L \subset \mathbb{R}^n$, its GSO $\mathbf{B}^\star$, and a target point $\mathbf{t} \in \mathbb{R}^n$.
Output: A decomposition $\mathbf{t} = (\mathbf{v} + \mathbf{f})$ where $\mathbf{v} \in L$ and $\mathbf{w} \in \mathcal{P}(\mathbf{B}^\star)$

$\mathbf{f} \leftarrow \mathbf{t}$
$\mathbf{v} \leftarrow \mathbf{0}$
for $i = n$ downto 1 **do**
  $y \leftarrow \langle \mathbf{t}, \mathbf{b}_i^\star \rangle / \|\mathbf{b}_i^\star\|^2$
  $z_i = \lfloor y \rceil$
  $\mathbf{f} \leftarrow \mathbf{f} - z_i \mathbf{b}_i$
  $\mathbf{v} \leftarrow \mathbf{v} + z_i \mathbf{b}_i$
return $(\mathbf{v}, \mathbf{f})$

Proof: The details are left as an exercise. For the first statement, one should use the Pythagorean identity, exploiting the orthogonality of the basis $\mathbf{B}^\star$. For the second identity, on should prove that the ball of radius d is included in $\mathcal{P}(\mathbf{B}^\star)$. □

6 Good bases, bad bases, and cryptography

As we have seen above, the ability to solve the δ-CVP and η-BDD problems highly depends on the quality of the basis that one is given. And it is also a hard problem, given bad basis of a lattice to construct a good one. But one thing that can be done, is to directly construct a lattice L as the lattice $\mathcal{L}(\mathbf{G})$ for some good basis $\mathbf{G}$ that one chooses !

This very idea gives a foundation to build asymmetric cryptography from lattices. It goes as follows:

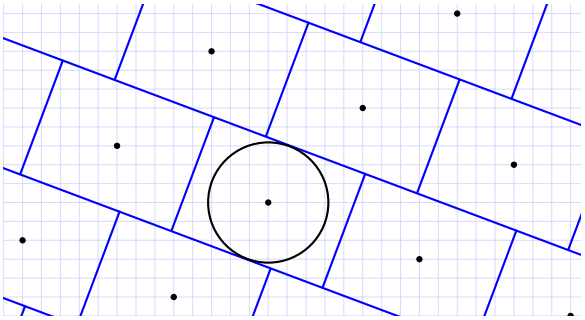
- Alice chooses a good basis $\mathbf{G}$, and set $L = \mathcal{L}(\mathbf{G})$. She keeps $\mathbf{G}$ as a *secret key* $sk = \mathbf{G}$.
- She also derives $\mathbf{B}$ a bad basis of the same lattice: $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{G})$.[6] She makes $pk = \mathbf{B}$ public as her *public key*.
- Bob uses $\mathbf{B}$ to encrypt messages
- Alice uses $\mathbf{G}$ to decrypt messages.

But how are messages encrypted and decrypted ? Well, we need to have a gap between the quality of $\mathbf{B}$ and $\mathbf{G}$. Let η be a positive real number such that:

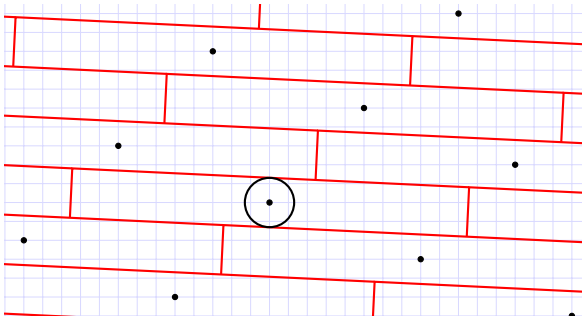
$$\eta_{\mathbf{B}} = \frac{1}{2} \min \|\mathbf{b}_i^\star\| \ll \eta \leq \frac{1}{2} \min \|\mathbf{g}_i^\star\| = \eta_{\mathbf{G}}.$$

[6] This can be done for example by sampling a random unimodular matrix $\mathbf{U}$ and setting $\mathbf{B} = \mathbf{GU}$. There are better ways to do that, see the Hermite normal form in the lecture X from XXX

Figure 5: BDD radius using $\mathbf{G}$ versus $\mathbf{B}$



Decoding radius with $\mathbf{G}^\star$



Decoding radius with $\mathbf{B}^\star$

The symbol $\ll$ means "much smaller than", and it won't be made formal in this lecture. The reason we need a significant margin is that the nearest plane Algorithm behave better in the average case than in the worst case: the sufficient condition of Proposition 7 are not exactly necessary in the average case.

With those conditions, Alice will be able to solve η-BDD while this will be very hard for anyone else knowing only $\mathbf{B}$. This suggest to make the ciphertext an η-BDD instance, so that only alice can solve it !

More precisely, one would define the encryption function on a message $\mathbf{m} \in \{0,1\}^n$ (the message is viewed as a vector of bits) and with the public key $pk = \mathbf{B}$ to obtain a ciphertext $\mathbf{c}$ as follows:

$$\mathbf{c} = \mathcal{E}(\mathbf{B}, \mathbf{m}) = \mathbf{B} \cdot \mathbf{m} + \mathbf{e}$$

where $\mathbf{e}$ is a random vector of length η: $\|\mathbf{e}\| = \eta$.

The decryption function will use the Nearest Plane algorithm to remove the error $\mathbf{e}$. Alice will use both the good and the bad basis to recover the message.

$$\mathbf{m}' = \mathcal{D}(\mathbf{G}, \mathbf{B}, \mathbf{c}) = \mathbf{B}^{-1}\mathbf{v} \quad \text{where } (\mathbf{v}, \mathbf{e}') = \text{NearestPlane}(\mathbf{G}, \mathbf{G}^\star, \mathbf{c}).$$

Using Proposition 7, one deduce that $\mathbf{m}' = \mathbf{m}$: Alice has properly decrypted the ciphertext $\mathbf{c}$ to the message right message $\mathbf{m}$.

Is the above scheme truly secure ? We have informally argued that, without the secret key $sk = \mathbf{G}$, it should be hard to recover the message $\mathbf{m}$. This is unfortunately not so simple, and it is possible to attack this scheme. To see this, one need to start studying what it means precisely for a scheme to be secure in a formal sense, which is left as an exercise for the curious reader.

Problem 2 *Learn about the notion of Indistinguishability under Chosen-Plaintext Attacks (IND-CPA security), and show that the above scheme is not IND-CPA secure.*

7 Provably secure encryption from lattices and beyond

This lecture meant to give the basic tools to understand lattices, associated algorithms, and the ideas behind lattice based cryptography. Those ideas dates back from the early schemes of Goldreich-Goldwasser-and Halevi and the NTRU schemes (form the late 90').

Since then, the theory of lattice based cryptography has made tremendous progress, in particular by formalizing more precise problems called the Short-Integer-Solution problem (SIS) and the Learning-with-Error problem (LWE). Those problems are intrinsically lattice problems, but are typically presented without speaking of lattices at all ! While this is convenient to build better cryptosystems, this hides a little bit the intuition behind the design of those schemes.

Therefore, we shall finish this lecture with the translation of the LWE problem to a BDD problem.

Definition 10 (The Learning with Errors Problem) *The Learning with Errors Problem, $LWE_{n,m,q,\chi}$, with n unknown, $m \geq n$ samples, modulo q and with errors distribution χ is as follows:*

- *for a random secret $\mathbf{s}$ uniformly chosen in $\mathbb{Z}_q^n$,*
- *given m samples of the form $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e \bmod q)$ where $e \leftarrow \chi$ and $\mathbf{a}$ is uniform in $\mathbb{Z}_q^n$,*
- *recover the secret vector $\mathbf{s}$.*

To state this problem in term of lattice, consider the matrix $\mathbf{A} = [\mathbf{a}_1 \dots \mathbf{a}_m]^t$ whose rows are the samples $\mathbf{a}_i$, the vector $\mathbf{b} = \mathbf{As} + \mathbf{e}$ where $\mathbf{e} \leftarrow \chi^m$, and define the LWE lattice.

Definition 11 (The LWE-lattice) *For integers parameters $n, m > n, q$, and for a $LWE_{n,m,q,\cdot}$ instance matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, the LWE-lattice associated to the instance $(\mathbf{A}, \mathbf{b})$, $\mathcal{L}^q(\mathbf{A}^t)$, is defined as:*

$$\mathcal{L}^q(\mathbf{A}) = \left\{ \mathbf{v} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}_q^n s.t. \, \mathbf{v} \equiv \mathbf{As} \bmod q \right\}.$$

In other words, $\mathcal{L}^q(\mathbf{A})$ is the lattice generated by the column vectors of $\mathbf{A}$ and the column vectors of $q\mathbf{I}_m$, i.e. *the canonical vectors scaled by q.*

When $\mathbf{e}$ is small, the problem can now be seen as follows: given a point $\mathbf{b}$ close to a random lattice point $\mathbf{As} \bmod q$, one is asked to recover $\mathbf{s}$. The problem LWE is a variant of BDD for a certain distribution of lattice and errors. We will conclude with the following exercise:

Problem 3 *Prove that for any matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, $\mathcal{L}^q(\mathbf{A})$ is a lattice, that it has dimension m and volume q^{m-n}.*

Hint: For the volume, first prove that if L' is a sublattice L, then the quotient group L/L' has size $\mathrm{Vol}(L')/\mathrm{Vol}(L)$.