Lecture Notes: Preliminaries of Module-Lattice-Based Key-Encapsulation Mechanism

Ji, Yong-Hyeon

September 30, 2024

Contents

1 Introduction

In this lecture, we will cover the preliminary concepts for understanding Module-Lattice-based Key Encapsulation Mechanisms (KEM). To make abstract concepts more accessible, each definition will be followed by several concrete examples and observations, with visualizations. This will help bridge the gap between abstract theory and intuitive understanding.

2 Linear Algebra and Euclidean Lattices

2.1 Vectors and Vector Spaces

Definition 1 *A **vector space** V over a field $\mathbb{F}$ is a set of vectors where two operations are defined:*

- *Vector addition:* $\mathbf{u} + \mathbf{v}$
- *Scalar multiplication:* $c \cdot \mathbf{v}$ *for* $c \in \mathbb{F}$

The space V is closed under these operations, meaning if you add two vectors or multiply a vector by a scalar, the result stays in V.

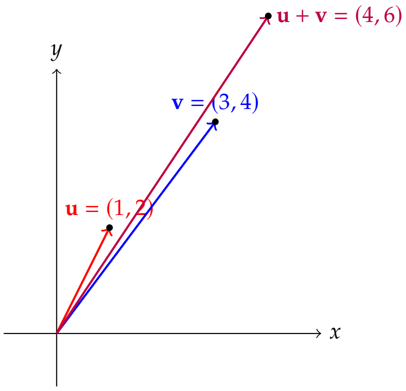
Example 1 *The space $\mathbb{R}^2$ consists of vectors of the form $\mathbf{v} = (v_1, v_2)$, where $v_1, v_2 \in \mathbb{R}$. An example of vector addition in $\mathbb{R}^2$:*

$$(1, 2) + (3, 4) = (4, 6).$$

Example 2 *The space $\mathbb{R}^3$ consists of vectors like $\mathbf{v} = (v_1, v_2, v_3)$. Consider the vector $\mathbf{v} = (1, -1, 2)$ and a scalar $c = 2$. Then scalar multiplication gives:*

$$2 \cdot (1, -1, 2) = (2, -2, 4).$$

Observation 1 *Vector spaces are abstractions that generalize the familiar idea of points and lines in 2D and 3D spaces. Working with $\mathbb{R}^2$ and $\mathbb{R}^3$ as concrete examples helps ground the abstract notion of higher-dimensional vector spaces.*



2.2 Lattices in Vector Spaces

Definition 2 *A* ***lattice*** Λ *in a vector space* $\mathbb{R}^n$ *is a set of points formed by all integer linear combinations of a set of linearly independent vectors,* $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$.

$$\Lambda = \left\{ \sum_{i=1}^{n} z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}.$$

Here, $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ *is called a* ***basis*** *of the lattice.*

Example 3 *In* $\mathbb{R}^2$*, let* $\mathbf{b}_1 = (1, 0)$ *and* $\mathbf{b}_2 = (0, 1)$*. The lattice generated by these vectors is* $\mathbb{Z}^2$*, which consists of all points with integer coordinates, i.e.,*

$$\Lambda = \{(z_1, z_2) : z_1, z_2 \in \mathbb{Z}\}.$$

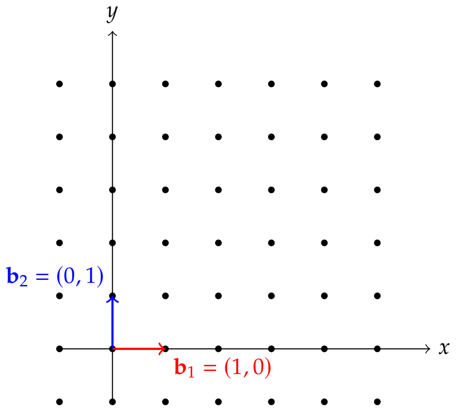
For example, $(2, 3) \in \Lambda$*, and* $(\frac{1}{2}, 1) \notin \Lambda$.

Example 4 *Consider the vectors* $\mathbf{b}_1 = (2, 0)$ *and* $\mathbf{b}_2 = (0, 2)$ *in* $\mathbb{R}^2$*. The lattice generated by these vectors is a scaled version of* $\mathbb{Z}^2$*, consisting of points with even integer coordinates:*

$$\Lambda = \{(2z_1, 2z_2) : z_1, z_2 \in \mathbb{Z}\}.$$

Thus, points like $(2, 4)$ *are in the lattice, but* $(1, 3)$ *is not.*

Observation 2 *Lattices can be visualized as grids of points. The vectors used to generate the lattice define the spacing and structure of the grid. Changing the basis vectors changes the grid's shape, but the fundamental lattice structure remains the same.*



2.3 Norms and Closest Vector Problem (CVP)

Definition 3 *The* ***Euclidean norm*** *of a vector* $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{R}^n$ *is the length of the vector, given by:*

$$\|\mathbf{v}\| = \sqrt{v_1^2 + v_2^2 + \cdots + v_n^2}.$$

Example 5 *For the vector* $\mathbf{v} = (3, 4)$ *in* $\mathbb{R}^2$*, the Euclidean norm is:*

$$\|\mathbf{v}\| = \sqrt{3^2 + 4^2} = \sqrt{9 + 16} = 5.$$

This is the length of the vector from the origin to the point $(3, 4)$.

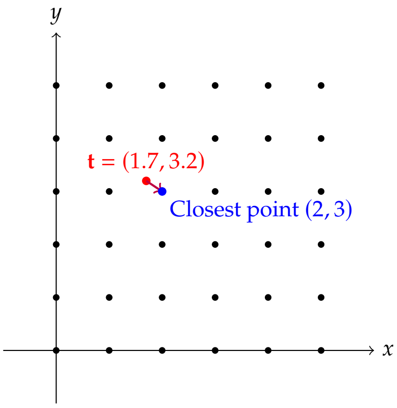
Definition 4 *The **Closest Vector Problem (CVP)** asks: Given a lattice $\Lambda \subset \mathbb{R}^n$ and a target point $\mathbf{t} \in \mathbb{R}^n$, find the lattice point $\mathbf{v} \in \Lambda$ that is closest to $\mathbf{t}$ in terms of Euclidean distance.*

Example 6 *Let $\Lambda = \mathbb{Z}^2$ and the target point be $\mathbf{t} = (1.7, 3.2)$. The closest lattice point in Λ is $(2, 3)$ because:*

$$\|(1.7, 3.2) - (2, 3)\| = \sqrt{(1.7 - 2)^2 + (3.2 - 3)^2} = \sqrt{0.09 + 0.04} = \sqrt{0.13}.$$

This is smaller than the distance to any other lattice point.

Observation 3 *The CVP is intuitively about finding the nearest "grid point" to a given point. Although this seems easy in low dimensions (like 2D), it becomes computationally hard in high dimensions, which makes it suitable for cryptographic applications.*



3 Introduction to Modules

3.1 Rings

Definition 5 *A **ring** R is a set with two operations: addition and multiplication. It satisfies properties similar to the integers, including distributivity of multiplication over addition. Examples of rings include $\mathbb{Z}$ and $\mathbb{Z}_q$ (integers modulo q).*

Example 7 *Consider the ring $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Addition and multiplication are performed modulo 5:*

$$2 + 4 = 1 \pmod 5, \quad 3 \times 4 = 2 \pmod 5.$$

Example 8 *The ring $\mathbb{Z}$ (integers) supports familiar operations:*

$$2 + 3 = 5, \quad 4 \times 5 = 20.$$

However, $\mathbb{Z}$ has no bounds like $\mathbb{Z}_5$, which loops back when reaching 5.

Observation 4 *Rings generalize the structure of numbers under addition and multiplication. Familiar rings like integers and modular integers are foundational to many cryptographic constructions.*

4 Conclusion

In this lecture, we introduced lattice and module lattice concepts, grounding them in several concrete examples and visualizations. These ideas form the foundation for Module-Lattice-based Key Encapsulation Mechanisms (KEMs), which we will explore in more detail in the following lectures.

5 Module Lattices and Cryptographic Applications

Lattice-based cryptography is an important area of post-quantum cryptography, and module lattices provide an efficient and flexible framework for building cryptographic schemes. In this section, we introduce the concept of module lattices step by step, using examples to make the abstract theory clearer and visualizations to build an intuitive understanding of these structures.

5.1 Module Lattices

Definition 6 *A* ***module lattice*** *is a lattice that is also a module over some ring R. Formally, it consists of integer linear combinations of basis vectors, but the coefficients come from the ring R rather than the integers.*

5.1.1 Step-by-Step Explanation

To understand module lattices, let's break down the key components:

- **Lattice**: A lattice is a grid of points generated by integer combinations of basis vectors. The simplest example is the integer lattice $\mathbb{Z}^2$, which can be visualized as a regular grid of points in the plane.
- **Module over a ring**: A module generalizes vector spaces by allowing the coefficients (scalars) to come from a ring, rather than a field. Rings allow operations like addition and multiplication, but without requiring division.
- **Module Lattice**: In a module lattice, the grid-like structure of a lattice is combined with the algebraic structure of a module over a ring.

5.2 Example 1: Module Lattice over $\mathbb{Z}_5$

Let's begin with a concrete example to make this more intuitive.

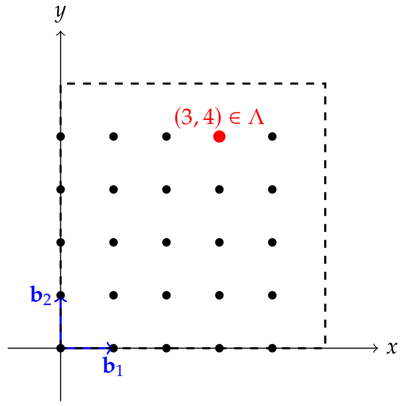
Example 9 *Consider the ring* $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ *(integers modulo 5) and the vectors* $\mathbf{b}_1 = (1, 0)$, $\mathbf{b}_2 = (0, 1)$ *in* $\mathbb{R}^2$. *The module lattice over* $\mathbb{Z}_5$ *is formed by taking all combinations of* $\mathbf{b}_1$ *and* $\mathbf{b}_2$ *with coefficients from* $\mathbb{Z}_5$. *That is:*

$$\Lambda = \{z_1\mathbf{b}_1 + z_2\mathbf{b}_2 : z_1, z_2 \in \mathbb{Z}_5\} .$$

The points of the lattice are given by (z_1, z_2) *where* $z_1, z_2 \in \{0, 1, 2, 3, 4\}$.

For example, $(3, 4)$ *is in the lattice since* $z_1 = 3$ *and* $z_2 = 4$ *are elements of* $\mathbb{Z}_5$.

Observation 5 *In this example, the module lattice takes on a periodic structure because the coefficients are restricted to a finite set (modulo 5). This results in a finite number of points in the lattice, forming a grid structure within a bounded region. The periodicity of the lattice can be visualized as repeating blocks of points.*



5.3 Example 2: Module Lattice over $\mathbb{Z}_7$

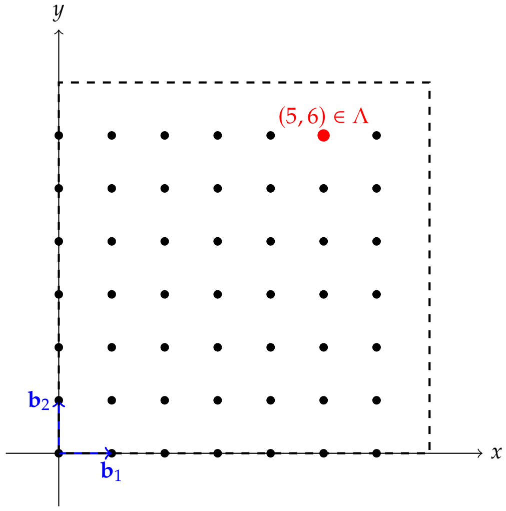
Example 10 *Now consider the ring $\mathbb{Z}_7$ (integers modulo 7) and the same basis vectors $\mathbf{b}_1 = (1, 0)$ and $\mathbf{b}_2 = (0, 1)$ in $\mathbb{R}^2$. The module lattice over $\mathbb{Z}_7$ is given by:*

$$\Lambda = \{z_1\mathbf{b}_1 + z_2\mathbf{b}_2 : z_1, z_2 \in \mathbb{Z}_7\}.$$

The points of the lattice are given by (z_1, z_2) where $z_1, z_2 \in \{0, 1, 2, 3, 4, 5, 6\}$.

For example, $(5, 6)$ is in the lattice because $z_1 = 5$ and $z_2 = 6$ are elements of $\mathbb{Z}_7$.

Observation 6 *In this example, the periodicity is different because the coefficients come from $\mathbb{Z}_7$. This creates a larger, more spread-out grid of points, compared to the previous example. The concept of using different rings ($\mathbb{Z}_5$, $\mathbb{Z}_7$, etc.) allows for modular arithmetic that creates different lattice structures.*



5.4 Example 3: Non-Standard Basis Vectors

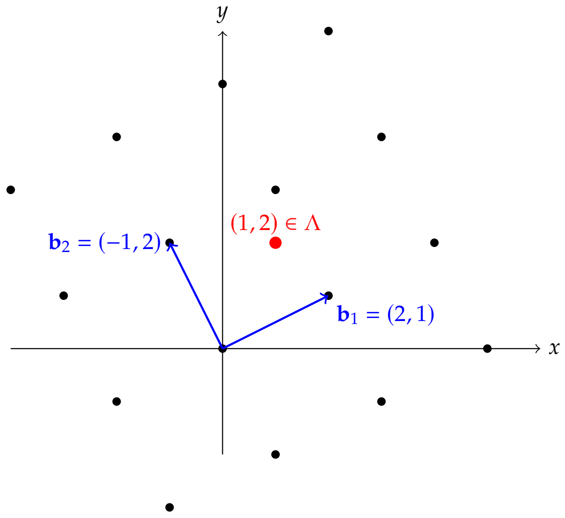
Example 11 *Let's now change the basis vectors to something less standard. Consider the ring $\mathbb{Z}_3$ and the basis vectors $\mathbf{b}_1 = (2, 1)$ and $\mathbf{b}_2 = (-1, 2)$. The module lattice over $\mathbb{Z}_3$ is given by:*

$$\Lambda = \{z_1\mathbf{b}_1 + z_2\mathbf{b}_2 : z_1, z_2 \in \mathbb{Z}_3\}.$$

Here, the lattice points will form a more skewed grid due to the non-standard choice of basis vectors.

For example, the point $(1, 2)$ can be written as $1\mathbf{b}_1 + 2\mathbf{b}_2 = (1, 2)$.

Observation 7 *Changing the basis vectors changes the shape of the grid. Instead of forming a standard rectangular grid, the points now form a rhombus-like pattern. The flexibility in choosing basis vectors and rings allows for different lattice structures, which can be tailored to specific cryptographic applications.*



6 Conclusion

In this lecture, we introduced the concept of module lattices and illustrated how these structures are formed by combining lattices and modules over rings. We explored several concrete examples and visualized them using different rings and basis vectors. These examples show the flexibility of module lattices in forming different grid structures, which are essential in cryptographic constructions.