

Introduction to Lattices in Cryptography

Dr. Essam Ghadafi

CyBOK © Crown Copyright, The National Cyber Security Centre 2025, licensed under the Open Government Licence <http://www.nationalarchives.gov.uk/doc/open-government-licence/>

CyBOK MAPPING

The lecture maps to the following CyBOK Knowledge Areas:

- Systems Security → Cryptography
- Infrastructure Security → Applied Cryptography

CyBOK

ESSAM GHADAFI

2

OUTLINE

- **A brief Overview of Vectors and Matrices:** Basic concepts of vectors and matrices, essential for understanding lattices
- **Definition of Lattices:** What is a lattice? Examples and intuition
- **Lattice Basis:** How lattices are generated from basis vectors
- **Determinant/Volume of a Lattice:** Fundamental parallelepiped and its significance
- **Geometry of Lattices:** Orthogonality and geometric properties
- **Successive Minima of a Lattice:** Understanding lattice structure

CyBOK

ESSAM GHADAFI

3

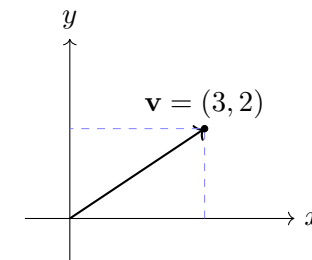
VECTORS

A vector is an ordered list of numbers that represents a point or a direction in space

- A 2D vector is written as $\mathbf{v} = (v_1, v_2)$
- A nD vector is written as $\mathbf{v} = (v_1, v_2, \dots, v_n)$

Vectors can be thought of as arrows pointing from one position to another

Example:



CyBOK

ESSAM GHADAFI

4

VECTOR LENGTH (P-NORM)

The length (or norm) of a vector is a way to measure its size. The general formula is:

$$\|\mathbf{v}\|_p = (|v_1|^p + |v_2|^p + \dots + |v_n|^p)^{\frac{1}{p}}$$

Special cases of the p-norm:

- **Euclidean Norm** ($L_2, p = 2$): $\|\mathbf{v}\|_2 = \sqrt{v_1^2 + v_2^2 + \dots + v_n^2}$
- **Manhattan Norm** ($L_1, p = 1$): $\|\mathbf{v}\|_1 = |v_1| + |v_2| + \dots + |v_n|$
- **Maximum Norm** ($L_\infty, p \rightarrow \infty$):
 $\|\mathbf{v}\|_\infty = \max(|v_1|, |v_2|, \dots, |v_n|)$

The Euclidean norm is the default, and we will denote it by just $\|\cdot\|$

Example:

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

MATRIX

A matrix is a rectangular array of numbers, arranged in rows and columns

$$\mathbf{M} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

- A matrix with m rows and n columns is called an $m \times n$ matrix
- **Special cases:**
 - A square matrix has the same number of rows and columns
 - A diagonal matrix has nonzero elements only on its diagonal
 - The identity matrix \mathbf{I} has ones on the diagonal and zeros elsewhere

MATRIX MULTIPLICATION

You can only multiply compatible matrices

Rule: The number of columns in the LHS matrix must equal the number of rows in the RHS matrix

Example: Matrix multiplication of a 2×2 matrix with a 2×1 matrix (column vector):

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \times \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_{11}b_1 + a_{12}b_2 \\ a_{21}b_1 + a_{22}b_2 \end{bmatrix}$$

Remember: Multiplying a matrix by its inverse results in the identity matrix:

$$\mathbf{A} \times \mathbf{A}^{-1} = \mathbf{A}^{-1} \times \mathbf{A} = \mathbf{I}$$

LATTICE DEFINITION – INTUITION

Lattice: A set of points in n-dimensional space that exhibits a periodic structure, i.e. **A lattice is just a grid of points**

Intuition: The lattice is an infinite grid of points arranged in a regular, repeating pattern that extends in multiple dimensions

- The position of each point is determined by the lattice basis
- The basis vectors define the directions and distances to reach the lattice points

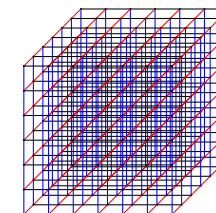


FIGURE: An example of 3D Lattice

WHY LATTICE-BASED CRYPTOGRAPHY?

- Provable security from worst-case assumptions
 - Stronger security guarantees
- Lattice-based assumptions (e.g., LWE, SIS) are “believed” to be quantum-resistant
- Widely used, e.g. NIST PQC candidates are mostly lattice-based
- Efficiency
 - Works over matrices and rings, it mostly involves addition and multiplication so no modular exponentiations or pairings
- Relatively more mature than some other PQC approaches

LATTICE DEFINITION

Working over \mathbb{R}^n , an n -dimensional lattice L is an (additive) discrete subgroup of \mathbb{R}^n , consisting of n -dimensional vectors from \mathbb{R}

- **Additive:** For all $x \in L$, $-x \in L$, and for all $x, y \in L$, $x + y \in L$
 - Adding/subtracting points in the lattice, results in another lattice point
- **Discrete:** Points are sufficiently far apart
- **Subgroup:** A subset that is a group under addition

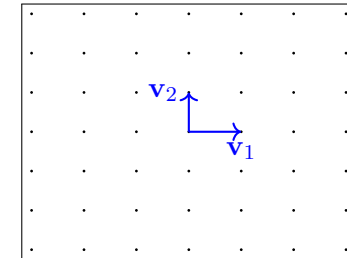


FIGURE: Example 2D lattice

LATTICE BASIS – INTUITION

💡 **Intuition:** The basis of a lattice defines the directions (or vectors) you can use to reach any point in the grid

- Each point in the lattice (grid) can be reached by combining the basis vectors, using some integer multiples

LATTICE BASIS – INTUITION

Example: Consider the 2D lattice generated by the basis $b_1 = (2, 1)$ and $b_2 = (1, 3)$

- Point $(3, 4)$ (in red) is obtained as $b_1 + b_2$
- Point $(5, 5)$ (in blue) is obtained by $2b_1 + b_2$
- ...

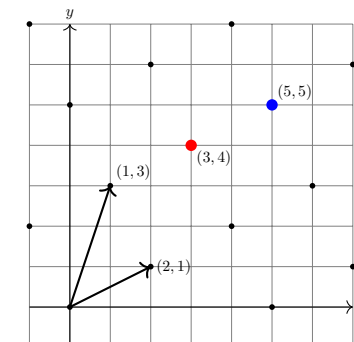


FIGURE: 2D-Lattice generated by the basis $b_1 = (2, 1)$ and $b_2 = (1, 3)$

LATTICE BASIS

A **basis** of a lattice is a set of k linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_k \in \mathbb{R}^n$ (points in the lattice) s.t. any vector \mathbf{v} in the lattice can be written as an integer linear combination of the basis vectors:

$$\mathbf{v} = \sum_{i=1}^k c_i \mathbf{b}_i, \quad c_i \in \mathbb{Z}$$

We can think of the basis as a matrix $\mathbf{B} \in \mathbb{R}^{n \times k}$ with k -linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_k \in \mathbb{R}^n$ as columns:

$$\mathbf{B} = \begin{bmatrix} \mathbf{b}_1 & \mathbf{b}_2 & \dots & \mathbf{b}_k \end{bmatrix}$$

We denote the lattice generated by the basis matrix $\mathbf{B} \in \mathbb{R}^{n \times k}$ by $L(\mathbf{B})$

MATHEMATICAL LATTICE

- $L(\mathbf{B})$ is a discrete set of points in \mathbb{R}^n that can be described as:

$$L(\mathbf{B}) = \left\{ \sum_{i=1}^k \alpha_i \mathbf{b}_i \mid \alpha_i \in \mathbb{Z} \right\}$$

where $\alpha_i \in \mathbb{Z}$ are integers.

Alternatively, we can define the lattice as:

$$L(\mathbf{B}) = \left\{ \mathbf{v} \in \mathbb{R}^n \mid \mathbf{v} = \mathbf{B}\boldsymbol{\alpha} \text{ for some } \boldsymbol{\alpha} \in \mathbb{Z}^k \right\}$$

LATTICE QUIZ

Quiz: Can you think of a matrix \mathbf{B} (of any size) with entries from \mathbb{R} that cannot serve as a lattice basis?

- **Hint:** The basis span does not form an additive discrete subgroup ...

LATTICE RANK

Lattice Rank is the number of vectors in its basis (i.e., k)

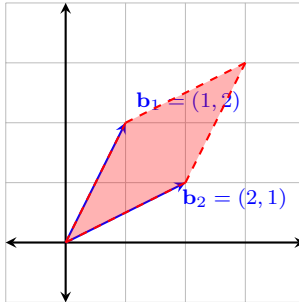
💡 **Intuition:** The rank is the number of independent directions needed to span the lattice space, i.e. to navigate the entire point grid

A lattice has **full rank** iff $k = n$, meaning it has a square basis matrix $\mathbf{B} \in \mathbb{R}^{n \times n}$ with **full rank** n , i.e., $\det(\mathbf{B}) \neq 0$.

FUNDAMENTAL PARALLELEPIPED – INTUITION

Intuition: The fundamental parallelepiped is the smallest region (box) formed by the lattice basis vectors, containing one lattice point and repeating throughout the lattice

- The smallest building block/tile of the point grid
- The lattice is created by shifting this tile in different directions, forming the entire point grid



CyBOK **FIGURE:** Fundamental parallelepiped of a 2D lattice with basis vectors $\mathbf{b}_1 = (1, 2)$ and $\mathbf{b}_2 = (2, 1)$ ESSAM GHADAFI

17

FUNDAMENTAL PARALLELEPIPED

Tiling of the lattice with its basis's fundamental parallelepiped

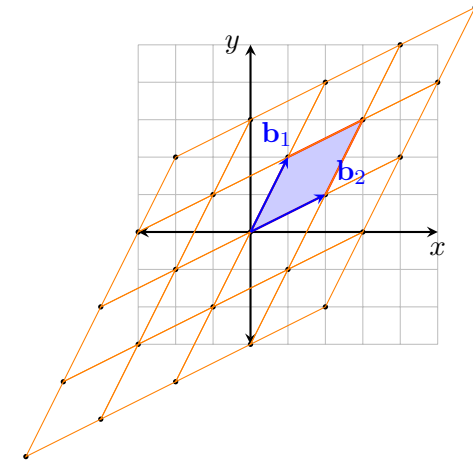


FIGURE: Tiling of the 2D lattice with basis vectors $\mathbf{b}_1 = (1, 2)$ and $\mathbf{b}_2 = (2, 1)$

CyBOK

ESSAM GHADAFI

18

FUNDAMENTAL PARALLELEPIPED

The **fundamental parallelepiped** of a basis matrix $\mathbf{B} \in \mathbb{R}^{n \times k}$ denoted by $\mathcal{P}(\mathbf{B})$ is the region of space spanned by \mathbf{B} where each point within the parallelepiped is a **convex combination** of the basis vectors with the coefficients λ_i satisfying $0 \leq \lambda_i < 1$

$$\mathcal{P}(\mathbf{B}) = \left\{ \sum_{i=1}^k \lambda_i \mathbf{b}_i \quad \text{with} \quad 0 \leq \lambda_i < 1 \right\}$$

The **volume** (or n-dimensional measure) of the fundamental parallelepiped is given by the absolute value of the determinant of the basis matrix:

$$\text{Volume} = |\det(\mathbf{B})|$$

FUNDAMENTAL PARALLELEPIPED

Some useful properties:

- \mathbf{B} can only be a basis for the lattice $L(\mathbf{B})$ if $\mathcal{P}(\mathbf{B})$ does not contain any points in $L(\mathbf{B})$ other than the origin, i.e. $L(\mathbf{B}) \cap \mathcal{P}(\mathbf{B}) = \{\mathbf{0}\}$
- $L(\mathbf{B})$ can be fully tiled by placing $\mathcal{P}(\mathbf{B})$ at each point in $L(\mathbf{B})$ (as we have seen earlier)

DETERMINANT (VOLUME) OF LATTICE

The **determinant** of a lattice classifies the lattice density (how spread out the points are):

- A larger determinant \Rightarrow a more “spread-out” lattice (lower density)
- A smaller determinant \Rightarrow a denser packing of lattice points (higher density)

For a lattice $L(\mathbf{B}) \subseteq \mathbb{R}^n$, the determinant (volume) of the lattice is $\det(L(\mathbf{B})) = \text{Volume}(\mathcal{P}(\mathbf{B})) = |\det(\mathbf{B})| \leq \prod_{i=1}^k \|\mathbf{b}_i\|$

LATTICE BASIS

An n -dimensional lattice, for $n > 1$, will have infinitely many bases that can generate it

Two matrices $\mathbf{B} \in \mathbb{R}^{n \times n}$ and $\mathbf{B}' \in \mathbb{R}^{n \times n}$ are bases for the same lattice (i.e. generate the same lattice) if and only if

$$\mathbf{B} = \mathbf{B}'\mathbf{U}$$

for some unimodular matrix $\mathbf{U} \in \mathbb{R}^{n \times n}$, where $|\det(\mathbf{U})| = 1$

This means we have

$$\det(\mathbf{B}) = \pm \det(\mathbf{B}')$$

This means the volume of a parallelepiped formed by the lattice basis vectors is invariant, i.e. $\text{Volume}(\mathcal{P}(\mathbf{B})) = \text{Volume}(\mathcal{P}(\mathbf{B}'))$

Note: The same applies when the lattice is not full rank (when the basis matrix is not square)

LATTICE BASIS

Example: Consider the lattice in \mathbb{R}^2 generated by the basis:

$$\mathbf{B}_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Another valid basis for the same lattice is

$$\mathbf{B}_2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

We have

$$\mathbf{B}_2 = \mathbf{B}_1\mathbf{U}$$

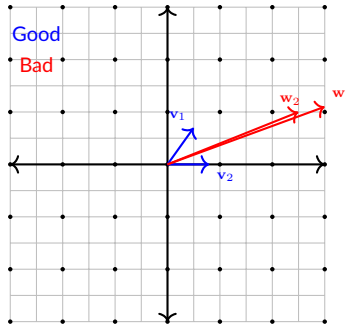
where

$$\mathbf{U} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

LATTICE BASIS – THE GOOD, THE BAD

💡 Intuition:

- A good lattice basis has clear, direct steps, making it easy to navigate and quickly reach any point in the grid.
 - Used as a secret key in lattice-based cryptosystems
- A bad basis still reaches all points, but is inefficient, requiring unnecessary steps and complicating navigation.
 - Used as a public key in lattice-based cryptosystems



One can classify the basis as **Good** or **Bad**:

- **Good**: Consists of short, nearly orthogonal vectors, making computations more efficient and problem-solving easier
- **Bad**: Consists of long and highly skewed vectors (almost parallel), making the lattice computationally difficult to work with

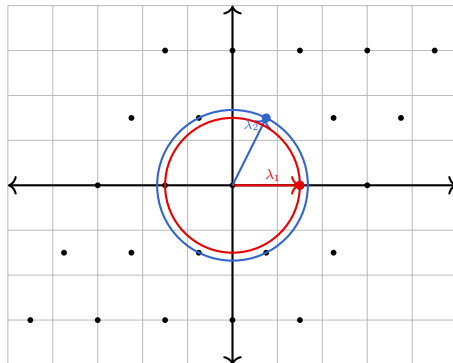
How to go from **bad** to **good**?

Transforming a **bad** basis to a better one involves shortening vectors and improving orthogonality among them

- **Gram-Schmidt**: Orthogonal but unstable and order-dependent
 - Does not always return a valid lattice basis
- **LLL (Lenstra-Lenstra-Lovász)**: Efficient (poly-time), produces shorter, nearly orthogonal vectors. Utilises Gram-Schmidt Orthogonalisation
- **BKZ (Block Korkine-Zolotarev)**: Improves LLL with block reduction, better results but higher cost

SUCCESSIVE MINIMA

💡 **Intuition**: The successive minima of a lattice measure how spread out the lattice is by identifying the smallest radii that enclose at least k independent vectors (points)



SUCCESSIVE MINIMA

The i -th **successive minimum** $\lambda_i(L(\mathbf{B}))$ of a lattice $L(\mathbf{B}) \subseteq \mathbb{R}^n$ is the smallest radius r s.t. i linearly independent vectors $\{\mathbf{v}_1, \dots, \mathbf{v}_i\}$ of length $\leq r$ exist, i.e. $\|\mathbf{v}_j\| \leq r$ for all $j = 1, \dots, i$.

$$\lambda_i(L(\mathbf{B})) = \inf\{r > 0 \mid \dim(\text{span}(L(\mathbf{B}) \cap B(0, r))) \geq i\}$$

Where:

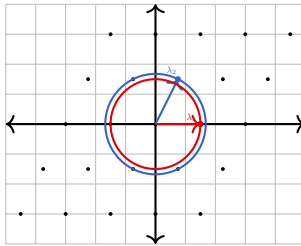
- $B(0, r)$ denotes the closed ball centered at the origin with radius r
- $L(\mathbf{B}) \cap B(0, r)$ is the set of lattice points contained within this ball

Note: \inf denotes the infimum: the largest number that is \leq every element of the set.

SUCCESSIVE MINIMA

- $\lambda_1(L(\mathbf{B}))$ is the length of the shortest nonzero vector in $L(\mathbf{B})$
 - The shortest vector is not unique, e.g. $\|\mathbf{v}\| = \|-\mathbf{v}\|$
- $\lambda_2(L(\mathbf{B}))$ is the **radius** of the smallest ball containing two linearly independent vectors
- In general, $\lambda_i(L(\mathbf{B}))$ is the **radius** of the smallest ball containing i linearly independent lattice vectors

The λ_n -ball contains a basis for an n -dimensional lattice



MINIMUM DISTANCE OF A LATTICE

The **minimum distance** of a lattice L , denoted by $\lambda(L)$, is the shortest distance between any two points in the lattice. It answers the question:

- **Q:** How close are the closest two points in the grid?

Formally,

$$\lambda(L) = \min_{\mathbf{v}, \mathbf{w} \in L, \mathbf{v} \neq \mathbf{w}} \|\mathbf{v} - \mathbf{w}\|$$

The lattice minimum distance is also the length of its shortest non-zero vector: $\lambda(L) = \lambda_1(L)$

Note: Since lattice points are discrete, the minimum distance must be > 0 , as otherwise the set would not be discrete and would not form a lattice

DUAL LATTICE

The **dual** (or **reciprocal**) **lattice** L^* of a lattice $L \subseteq \mathbb{R}^n$ is defined as:

$$L^* = \{\mathbf{y} \in \mathbb{R}^n \mid \mathbf{y}^T \mathbf{x} \in \mathbb{Z}, \quad \forall \mathbf{x} \in L\}$$

That is, the dual lattice consists of all vectors in \mathbb{R}^n that have an integer inner product with every vector L

The basis of L^* is given by:

$$\mathbf{B}^* = (\mathbf{B}^T)^{-1}$$

KEY TAKEAWAYS

- **Lattices** are discrete grids of points formed by integer combinations of basis vectors
- **The basis** of a lattice is not unique, but the determinant (volume of the fundamental parallelepiped) is invariant
 - Good lattice bases are short and nearly orthogonal; bad ones are long or nearly parallel, leading to inefficiency
- **The determinant** of a lattice represents the “density” of the lattice and plays a crucial role in geometry and applications
- **Successive minima** provide insights into the structure and density of the lattice

ADDITIONAL RESOURCES & READING

- <https://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf>
- https://link.springer.com/chapter/10.1007/978-3-642-23082-0_7
- https://link.springer.com/chapter/10.1007/978-3-540-88702-7_5