Lattice-Based Cryptography

Dhruman Gupta

December 8, 2025

Contents

1 Lattices

1.1 Basic Definitions

Definition 1 (Lattice)**.** *Let $v_1, \ldots, v_n \in \mathbb{R}^m$ be linearly independent vectors. The lattice generated by these vectors is*

$$L = L(v_1, \ldots, v_n) = \left\{ \sum_{i=1}^{n} a_i v_i \ : \ a_i \in \mathbb{Z} \right\}.$$

Any such set $\{v_1, \ldots, v_n\}$ that generates L is called a basis *of L, and n is the* dimension *of the lattice,* $\dim L = n$.

Definition 2 (Integer Lattice)**.** *A lattice $L \subseteq \mathbb{R}^m$ is an* integer lattice *if all vectors in L have integer coordinates. Equivalently, L is a subgroup of $\mathbb{Z}^m$ (for some $m \geq 1$).*

Integer lattices are especially convenient for computation.

1.2 Additive Subgroup Characterization

Definition 3 (Additive Subgroup)**.** *A subset $L \subseteq \mathbb{R}^m$ is an* additive subgroup *if it is closed under vector addition and subtraction: $v, w \in L \Rightarrow v \pm w \in L$.*

Definition 4 (Discrete Additive Subgroup)**.** *An additive subgroup $L \subseteq \mathbb{R}^m$ is* discrete *if there exists $\varepsilon > 0$ such that for all distinct $v, w \in L$,*

$$\|v - w\| \geq \varepsilon.$$

Proposition 1. *A subset $L \subseteq \mathbb{R}^m$ is a lattice if and only if it is a discrete additive subgroup of $\mathbb{R}^m$.*

1.3 Change of Basis Matrices

Let $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$ be two bases of the same lattice $L \subseteq \mathbb{R}^n$. Then, the change of basis matrix is an integer matrix $A \in \mathbb{Z}^{n \times n}$. More precisely:

$$(v_1, \ldots, v_n) = (w_1, \ldots, w_n)A.$$

A takes w to v, and A^{-1} takes v to w (the inverse exists as it takes a basis to a basis). In both cases, the coefficients of vectors must be integers, so A and A^{-1} are integer matrices. This implies that $det(A) = \pm 1$.

2 Fundamental Domains and Determinant

2.1 Fundamental Domain

Definition 5 (Fundamental Domain)**.** *Let $v_1, \ldots, v_n$ be a basis of a lattice $L \subseteq \mathbb{R}^m$. The* fundamental domain *corresponding to this basis is*

$$\mathcal{F}(v_1, \ldots, v_n) = \left\{ \sum_{i=1}^{n} t_i v_i \ : \ 0 \leq t_i < 1 \right\}.$$

Proposition 2. *Let $L \subseteq \mathbb{R}^m$ be an n-dimensional lattice. Every vector $x \in \mathbb{R}^m$ can be uniquely written as*

$$x = \ell + f,$$

where $\ell \in L$ and $f \in \mathcal{F}(v_1, \ldots, v_n)$ for any basis $v_1, \ldots, v_n$ of L.

Proof. Let $x \in \mathbb{R}^m$. We can write x as a linear combination of the basis vectors with real coefficients:

$$x = t_1 x_1 + \cdots + t_n x_n$$

for some $t_i \in \mathbb{R}$. Define $a_i = \lfloor t_i \rfloor$. Since $a_i \in \mathbb{Z}$ and $0 \leq t_i - a_i < 1$, we have

$$f = x - \sum_{i=1}^{n} a_i x_i \in \mathcal{F}(x_1, \ldots, x_n).$$

Furthermore,

$$\ell = \sum_{i=1}^{n} a_i x_i \in L.$$

Therefore,

$$x = f + \ell.$$

□

2.2 Determinant of a Lattice

Definition 6 (Determinant / Covolume)**.** *For an n-dimensional lattice $L \subseteq \mathbb{R}^m$, the* determinant *of L, denoted* $\det(L)$*, is the n-dimensional volume of any fundamental domain $\mathcal{F}(v_1, \ldots, v_n)$. It is also called the* covolume *of L.*

Proposition 3. *Let V be the $m \times n$ matrix whose columns are the basis vectors $v_1, \ldots, v_n$. When $m = n$ (i.e. $L \subseteq \mathbb{R}^n$ is full-dimensional), the volume of the fundamental domain is*

Proof. The volume of the fundamental domain is given by

$$\mathrm{vol}(\mathcal{F}) = \int_{\mathcal{F}} dx_1 \cdots dx_n.$$

To compute this integral, make the change of variables

$$(x_1, \ldots, x_n) = t_1 v_1 + \cdots + t_n v_n,$$

which can be written in matrix form as $x = Vt$.

Note that $\mathcal{F} = VC_n$, where $C_n = [0, 1]^n$. By the change of variables formula,

$$\mathrm{vol}(\mathcal{F}) = \int_{C_n} |\det(V)|\, dt_1 \cdots dt_n = |\det(V)|.$$

□

Corollary 1. *For a fixed lattice L, every fundamental domain (for different bases) has the same volume* $\det(L)$.

$$\operatorname{vol}\left(\mathcal{F}(v_1, \ldots, v_n)\right) = |\det(V)|.$$

Theorem 1 (Hadamard's Inequality)**.** *For any basis $v_1, \ldots, v_n$ of a lattice $L \subseteq \mathbb{R}^n$,*

$$\det(L) = \operatorname{vol}\left(\mathcal{F}\right) \leq \prod_{i=1}^{n} \|v_i\| .$$

Equality holds if and only if the basis vectors are mutually orthogonal.

3 Shortest and Closest Vector Problems

3.1 Exact Problems

Definition 7 (Shortest Vector Problem (SVP))**.** *Given a lattice L, find a non-zero vector*

$$v_{shortest} \in L \setminus \{0\}$$

of minimum Euclidean norm.

Definition 8 (Closest Vector Problem (CVP))**.** *Given a lattice $L \subseteq \mathbb{R}^m$ and a target $w \in \mathbb{R}^m$, find*

$$v_{closest} = \arg\min_{v \in L} \|w - v\| .$$

The solutions need not be unique. CVP is known to be NP-hard, and SVP is NP-hard under randomized reductions (under standard assumptions).

3.2 Other Related Problems

Definition 9 (Shortest Basis Problem (SBP))**.** *Given a lattice L, find a basis $v_1, \ldots, v_n$ that is "short" in some measure, e.g. minimizing* $\max_i \|v_i\|$ *or* $\sum_i \|v_i\|^2$.

Definition 10 (Approximate SVP)**.** *For an approximation factor $\gamma(n) \geq 1$, the γ-approximate SVP problem asks: given a lattice L of dimension n, find a non-zero $v \in L$ such that*

$$\|v\| \leq \gamma(n) \cdot \|v_{shortest}\| .$$

Definition 11 (Approximate CVP)**.** *For an approximation factor $\gamma(n) \geq 1$, given L and w, find $v \in L$ such that*

$$\|w - v\| \leq \gamma(n) \cdot \|w - v_{closest}\| .$$

3.3 Hermite's Theorem and Hermite Constant

Definition 12 (Hermite Constant)**.** *For dimension n, the* Hermite constant γ_n *is defined so that every lattice L of dimension n contains a non-zero vector v with*

$$\|v\|^2 \leq \gamma_n \cdot \det(L)^{2/n}.$$

Theorem 2 (Hermite's Theorem)**.** *For every n-dimensional lattice L there exists a non-zero vector $v \in L$ such that*

$$\|v\| \leq \sqrt{\gamma_n}\, \det(L)^{1/n}.$$

For large n, asymptotically

$$\frac{n}{2\pi e} \lesssim \gamma_n \lesssim \frac{n}{\pi e}.$$

3.4 Hadamard Ratio

Definition 13 (Hadamard Ratio)**.** *For a basis $B = (v_1, \ldots, v_n)$ of a lattice L,*

$$H(B) = \left(\frac{\det(L)}{\prod_{i=1}^{n} \|v_i\|} \right)^{1/n}.$$

We have $0 < H(B) \leq 1$ from the Hadamard inequality. The more orthogonal the basis B is, the closer $H(B)$ is to 1.

3.5 Minkowski's Theorem

Theorem 3 (Minkowski)**.** *Let $L \subseteq \mathbb{R}^n$ be an n-dimensional lattice and let $S \subseteq \mathbb{R}^n$ be a symmetric convex set (i.e. $x \in S \Rightarrow -x \in S$) such that*

$$\mathrm{vol}(S) > 2^n \det(L).$$

Then S contains a non-zero lattice vector, i.e. there exists $v \in L \setminus \{0\}$ with $v \in S$. If S is closed, the strict inequality can be replaced by $\geq$.

Proof. Let S be a symmetric convex set such that $\mathrm{vol}(S) > 2^n \det(L)$. Consider the set $\frac{1}{2}S$.

$$\mathrm{vol}\left(\frac{1}{2}S\right) = \left(\frac{1}{2}\right)^n \mathrm{vol}(S) > 2^n \det(L) \cdot \left(\frac{1}{2}\right)^n = \det(L).$$

Every vector $a \in \mathbb{R}^m$ can be uniquely written as $a = v + w$, where $w \in L$ and $v \in \mathcal{F}$ (the fundamental domain).

Define the map $f : \frac{1}{2}S \to \mathcal{F}$ by $f\left(\frac{1}{2}x\right) = w$, where w is the non-lattice part of $\frac{1}{2}x$. This map consists of finitely many translations by lattice vectors, and since S is bounded, f preserves volume.

Since $\mathrm{vol}(\frac{1}{2}S) > \mathrm{vol}(\mathcal{F})$, the map f cannot be injective. Therefore, there exist distinct points $\frac{1}{2}x, \frac{1}{2}y \in \frac{1}{2}S$ such that $f(\frac{1}{2}x) = f(\frac{1}{2}y) = w$.

Write $\frac{1}{2}x = v_1 + w$ and $\frac{1}{2}y = v_2 + w$ with $v_1 \neq v_2$. Then

$$\frac{1}{2}(x - y) = v_1 - v_2 \neq 0.$$

Since S is convex and symmetric, $\frac{1}{2}(x-y) \in S$. Thus S contains a non-zero lattice vector. □

By applying Minkowski's theorem to an n-dimensional hypercube of side length $2\det(L)$, one obtains Hermite's bound on the length of the shortest vector.

3.6 Gaussian Heuristic

Instead of a hypercube, one can consider an n-dimensional ball of radius r and approximate its volume. The *Gaussian heuristic* predicts that for a "random" n-dimensional lattice L,

$$\lambda_1(L) \approx \sigma(L) := \sqrt{\frac{n}{2\pi e}}\,\det(L)^{1/n},$$

meaning the shortest vector length is close (up to small constant factors) to this value, with high probability.

4 Babai's Algorithm

4.1 Orthogonal Bases

If a basis of L is orthogonal, many lattice problems are easy.
Let $v_1, \ldots, v_n$ be an orthogonal basis of L. Any $v \in L$ can be written uniquely as

$$v = \sum_{i=1}^{n} a_i v_i, \quad a_i \in \mathbb{Z}.$$

SVP with orthogonal basis. The shortest non-zero vector is simply the basis vector v_i of minimum length.

CVP with orthogonal basis. Given $w \in \mathbb{R}^n$, write

$$w = \sum_{i=1}^{n} t_i v_i, \quad t_i \in \mathbb{R}.$$

Then the closest lattice vector is

$$v = \sum_{i=1}^{n} a_i v_i, \quad a_i = \mathrm{round}(t_i).$$

4.2 Babai's Algorithm for Nearly Orthogonal Bases

For a basis that is *nearly* orthogonal (e.g. after lattice reduction), *Babai's rounding algorithm* gives an approximate solution to CVP.

Algorithm 1 Babai's Nearest-Plane Algorithm

Require: Basis $v_1, \ldots, v_n$ of a lattice L; target vector $w \in \mathbb{R}^n$
Ensure: Approximate closest lattice vector $v \in L$
1: Compute $t_1, \ldots, t_n \in \mathbb{R}$ such that $w = \sum_{i=1}^{n} t_i v_i$
2: **for** $i = 1$ to n **do**
3: $\quad a_i \leftarrow \text{round}(t_i)$
4: **end for**
5: **return** $v = \sum_{i=1}^{n} a_i v_i$

When the basis is sufficiently close to orthogonal, the returned v is often the closest lattice vector, or at least within a small approximation factor.

Analysis for how close v is to the actual vector is omitted.

5 Learning With Errors (LWE) and Hard Lattice Problems

5.1 The LWE Problem

Fix positive integers n (dimension) and $q \geq 2$ (modulus), and let χ be a probability distribution over $\mathbb{Z}_q$ (the "error distribution").

Let $s \in \mathbb{Z}_q^n$ be a secret vector. Define the distribution $A_{s,\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ by sampling

$$a \leftarrow \mathbb{Z}_q^n \text{ uniformly}, \qquad e \leftarrow \chi, \qquad b = \langle a, s \rangle + e \pmod{q},$$

and outputting (a, b).

Definition 14 (LWE with parameters (n, q, χ))**.** *An algorithm solves LWE if, given arbitrarily many independent samples from $A_{s,\chi}$ (for a fixed but unknown s), it can recover s with non-negligible probability.*

5.2 Some hardness results, and worst-case lattice problems

From here on, $\lambda_1(L)$ denotes the length of the shortest non-zero vector in L.

Definition 15 (GapSVP)**.** *Let L be a lattice. For a function $\beta(n)$ (the gap), the problem GapSVP_β asks, given L, to decide whether $\lambda_1(L) \leq 1$ or $\lambda_1(L) > \beta(n)$, under the promise that one of these is the case.*

LWE is believed to be at least as hard as approximating $\lambda_1(L)$ within polynomial factors for worst-case lattices (i.e. certain GapSVP and related problems), via classical and quantum reductions.

5.3 Small Integer Solution (SIS) Problem

SIS is often described as a "dual" of LWE.

Definition 16 (SIS)**.** *Let $A \in \mathbb{Z}_q^{n \times m}$ be a matrix whose columns $a_1, \ldots, a_m \in \mathbb{Z}_q^n$ are chosen uniformly at random. The SIS problem with parameter B asks for a non-zero integer vector $b = (b_1, \ldots, b_m) \in \mathbb{Z}^m$ such that*

$$Ab \equiv 0 \pmod{q} \quad \text{and} \quad \|b\| \leq B.$$

For appropriate ranges of q and B, solving SIS on average is as hard as solving certain worst-case lattice problems such as GapSVP and SIVP.

5.4 Shortest Independent Vectors Problem (SIVP)

Definition 17 (SIVP)**.** *Given an n-dimensional lattice L, find a set of n linearly independent lattice vectors $v_1, \ldots, v_n$ such that the maximum length $\max_i \|v_i\|$ is as small as possible among all bases of L.*

5.5 Bounded Distance Decoding (BDD)

Definition 18 (BDD)**.** *Let L be a lattice and $d > 0$. In the* bounded distance decoding *(BDD) problem, one is given a target x that is promised to be within distance d of the lattice:*

$$\exists\, v \in L : \|x - v\| \leq d.$$

The goal is to find this (or some) closest lattice vector v.

If $d < \lambda_1(L)/2$, then the closest vector is unique. BDD can be seen as a promise version of CVP in which the target is guaranteed to be close to the lattice.

5.6 Dual Lattice

Definition 19 (Dual Lattice)**.** *Let $L \subseteq \mathbb{R}^n$ be a lattice. The* dual lattice *L^* is defined as*

$$L^* = \{\, y \in \mathbb{R}^n : \langle y, x \rangle \in \mathbb{Z} \text{ for all } x \in L \,\}.$$

For example, for $t > 0$, the dual of $t\mathbb{Z}^n$ is $(1/t)\mathbb{Z}^n$.

5.7 Discrete Gaussian and SIVP

Definition 20 (Discrete Gaussian Distribution)**.** *Let L be a lattice and $r > 0$. The* discrete Gaussian *over L with parameter r assigns probability proportional to*

$$\exp\left(-\pi \frac{\|x\|^2}{r^2}\right)$$

to each $x \in L$ (properly normalized).

Typical samples from this distribution have norm around $r\sqrt{n}$ and are substantially longer than the shortest vector.

5.8 Reductions Relating LWE and Lattice Problems

Very roughly:

- GapSVP and SIVP reduce to BDD on certain lattices.
- BDD can in turn be reduced to LWE: given access to an LWE oracle, one can solve BDD within a radius on the order of $\lambda_1(L)/\text{poly}(n)$.
- Therefore, efficiently solving LWE (for typical parameters) would allow one to solve worst-case lattice problems like GapSVP and SIVP in (sub-)exponential regimes where no such algorithms are known.

6 An LWE-Based Public-Key Encryption Scheme

We now describe a (simplified) public-key encryption scheme based on LWE.

6.1 Parameters

These parameters are chosen so that decryption is possible, while maintaining good security.

- Dimension n.
- Prime modulus $q \in [n^2, 2n^2]$.
- Error distribution χ discrete normal distribution with variance αq.
- $\alpha = \frac{1}{\sqrt{(n)\log^2 n}}$
- $m = 1.1n \log q$

6.2 Key Generation

- Sample secret key
$$s \leftarrow \mathbb{Z}_q^n.$$
- Sample m (polynomial in n) LWE samples
$$(a_i, b_i) \leftarrow A_{s,\chi}, \quad i = 1, \ldots, m,$$
i.e. $a_i \leftarrow \mathbb{Z}_q^n$, $e_i \leftarrow \chi$ and $b_i = \langle a_i, s \rangle + e_i \pmod q$.
- Secret key:
$$\mathsf{sk} = s.$$
- Public key:
$$\mathsf{pk} = \{(a_i, b_i)\}_{i=1}^m.$$

6.3 Encryption

To encrypt a bit $x \in \{0,1\}$ using the public key $\{(a_i, b_i)\}$:

- Choose a random subset $S \subseteq \{1, \ldots, m\}$.
- Compute
$$a = \sum_{i \in S} a_i \pmod{q}, \qquad b' = \sum_{i \in S} b_i \pmod{q}.$$
- If $x = 1$, also add $\lfloor q/2 \rfloor$ to b':
$$b = \begin{cases} b' & \text{if } x = 0, \\ b' + \lfloor q/2 \rfloor \pmod{q} & \text{if } x = 1. \end{cases}$$
- The ciphertext is (a, b).

6.4 Decryption

Given ciphertext (a, b) and secret key s:

- Compute
$$t = b - \langle a, s \rangle \pmod{q}.$$
- Interpret t as an integer in $(-q/2, q/2)$ and output
$$\hat{x} = \begin{cases} 0 & \text{if } t \text{ is closer to 0 than to } \lfloor q/2 \rfloor, \\ 1 & \text{otherwise.} \end{cases}$$

6.5 Correctness

Each LWE sample satisfies
$$b_i = \langle a_i, s \rangle + e_i \pmod{q},$$
so for the chosen subset S we have
$$b = \sum_{i \in S} b_i = \left\langle \sum_{i \in S} a_i, s \right\rangle + \sum_{i \in S} e_i = \langle a, s \rangle + E \pmod{q},$$
where $E = \sum_{i \in S} e_i$ is the accumulated error. If $x = 0$ we send $b' = b$, and if $x = 1$ we send $b' = b + \lfloor q/2 \rfloor$.

On decryption,
$$t = c' - \langle a, s \rangle = \begin{cases} E & \text{if } b = 0, \\ E + \lfloor q/2 \rfloor & \text{if } b = 1, \end{cases} \pmod{q}.$$

So, we only have an error if $|E| \geq q/4$. Let's calculate the probability of this.

We sum of $\leq m$ terms, each with std αq, so std of $E \leq \sqrt{(}m)\alpha q < \frac{q}{\log n}$. χ is normal, so by Chernoff's bound:

$$\begin{aligned} P(|E| \geq \frac{q}{4}) &\leq 2e \exp(-\frac{q^2 \log^2 n}{4^2 2q^2}) \\ &= 2n^{-\frac{\log n}{32}} \end{aligned}$$

This is negligible, so decryption succeeds except with negligible probability.

6.6 Security

Let $\mathcal{U}$ be the uniform distribution over $\mathcal{Z}_q^n \times \mathcal{Z}_q$. I will state and prove the following lemmas, and then argue security.

Lemma 1. *Let $n \geq 1$, $2 \leq q \leq poly(n)$ a prime, and χ some distribution over $\mathcal{Z}_q$. Assume there exists a PPT adversary $\mathcal{A}$ that accepts w.p $1 - \epsilon_1(n)$ when $x \in A_{s,\chi}$, and rejects w.p $1 - \epsilon_2(n)$ when $x \in \mathcal{U}$, where $\epsilon_1(n), \epsilon_2(n) \in 2^{-\Omega(n)}$. Then, we can construct a PPT adversary $\mathcal{B}$ that can output s given samples from $A_{s,\chi}$ with non negligible probability.*

Proof. Let $s = (s_1, \ldots, s_n)$. I will show how to find s_1. Repeat the process for the rest. For all $k \in \mathbb{Z}_q$, consider the transformation $T_k : \mathbb{Z}_q^n \times \mathbb{Z}_q \to \mathbb{Z}_q^n \times \mathbb{Z}_q$ defined by:

$$T_k(a, b) = (a + (r, 0, \cdots, 0), b + rk)$$

where r is uniformly random in $\mathbb{Z}_q$.

Now, note that if $k = s_1$, then $T_k(A_{s,\chi}) = A_{s,\chi}$. If $k \neq s_1$, then $T_k(A_{s,\chi}) = \mathcal{U}$.

Use A to see whether $T_k(A_{s,\chi}) = A_{s,\chi}$. If so, then accept. Reject otherwise. There are only $poly(n)$ such k to try, so we can try them all. □

Lemma 2. *Let $n, q \geq 1$, χ some distribution over $\mathbb{Z}_q$. Assume there exists a PPT adversary $\mathcal{A}$ that can distinguish non-negligible samples of $A_{s,\chi}$ from $\mathcal{U}$. Then, we can construct a PPT adversary $\mathcal{B}$ that for all s, accepts $x \in A_{s,\chi}$ w.p exponentially close to 1, and rejects $x \in \mathcal{U}$ w.p exponentially close to 1.*

Proof. Let $t \in \mathbb{Z}_q^n$. Consider the transformation $f_t : \mathbb{Z}_q^n \times \mathbb{Z}_q \to \mathbb{Z}_q^n \times \mathbb{Z}_q$ defined by:

$$f_t(a, b) = (a, b + \langle t, a \rangle)$$

Note that $f_t(A_{s,\chi}) = A_{s+t,\chi}$, and $f_t(\mathcal{U}) = \mathcal{U}$.

Choose a t uniformly. Estimate the probability of acceptance of $\mathcal{A}$ on $f_t(A_{s,\chi})$ and $f_t(\mathcal{U})$ to degree $\pm\frac{1}{poly(n)}$.

If these differ, then it means that $f_t(\text{input}) = A_{s+t,\chi}$. So accept. Otherwise reject.

Now, repeat polynomially many times. If the input is indeed $A_{s,\chi}$, then we will get to some $A_{s+t,\chi}$ s.t $\mathcal{A}$ will distinguish between that and $\mathcal{U}$. So if we do not find that in polynomial time, then with probability exponentially close to 1, the input is not $A_{s,\chi}$. □

6.6.1 Proof that this is IndCPA

We are working under the assumption that with these parameters, the LWE problem is hard. We will show that this scheme is IndCPA secure under this assumption.

In the IndCPA game, the player sends two messages m_0, m_1 to the challenger, and then tries to distinguish between which one was encrypted. Since the messages in this setting are a bit, the game boils down to:

1. Challenger is given the public key.
2. $b \in \{0, 1\}$ is chosen uniformly, and encrypted to get c.
3. Challenger has to guess whether $b = 0$ or $b = 1$.

Say $\mathcal{A}$ is a PPT adversary that wins the game with probability $\frac{1}{2} + \epsilon(n)$ where ϵ is non-negligible.

Generate $(a_i, b_i)_{i=1}^m$ uniformly at random, instead of the LWE distribution. Now, for any subset S of this, the pair $(\sum_{i \in S} a_i, \sum_{i \in S} b_i)$ is almost uniformly random. The encryption of 0 and 1 are theoretically indistinguishable, so no adversary can distinguish them.

As $\mathcal{A}$ cannot distinguish between the two, we can use it to distinguish between the LWE distribution and the uniform distribution. Lemma 1 and 2 then imply that this adversary can break LWE.

This is contradicting our assumption that the LWE problem is hard. So, the scheme is IndCPA secure.

Summary

These notes have introduced:

- Two early cryptosystems (a toy scheme and Merkle's subset-sum scheme) that can be attacked via finding short vectors in lattices.
- Basic lattice theory, including bases, fundamental domains, and the determinant.
- Central computational problems (SVP, CVP, SIS, SIVP, BDD) and geometric tools (Minkowski, Hermite, Gaussian heuristic, Babai's algorithm).

- The Learning With Errors problem and its connection to worst-case lattice problems.
- A concrete LWE-based public-key encryption scheme, together with correctness and a sketch of its security based on LWE hardness.