LATTICES AND CRYPTOGRAPHY

Abderrahmane Nitaj

Laboratoire de Mathématiques Nicolas Oresme
University de Caen, France

Nouakchott, February 15-26, 2016

Contents

Contents

Introduction to lattices

Definition

Let n and d be two positive integers. Let $b_1 \cdots, b_d \in \mathbb{R}^n$ be d linearly independent vectors. The lattice $\mathcal{L}$ generated by $(b_1 \cdots, b_d)$ is the set

$$\mathcal{L} = \sum_{i=1}^{d} \mathbb{Z} b_i = \left\{ \sum_{i=1}^{d} x_i b_i \mid x_i \in \mathbb{Z} \right\}.$$

The vectors $b_1 \cdots, b_d$ are called a vector basis of $\mathcal{L}$. The lattice rank is n and the lattice dimension is d. If $n = d$ then $\mathcal{L}$ is called a full rank lattice.

Introduction to lattices

Notation

Let $b_1 \cdots, b_d \in \mathbb{R}^n$ and

$$\mathcal{L} = \sum_{i=1}^{d} \mathbb{Z} b_i = \left\{ \sum_{i=1}^{d} x_i b_i \mid x_i \in \mathbb{Z} \right\}.$$

We use vertical representation of the vectors.

$$\left[\begin{array}{c|c|c|c|c|c} b_1 & b_2 & \ldots & b_i & \ldots & b_d \\ \hline a_{11} & a_{12} & \ldots & a_{1i} & \ldots & a_{1d} \\ a_{21} & a_{22} & \ldots & a_{2i} & \ldots & a_{2d} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{j1} & a_{j2} & \ldots & a_{ji} & \ldots & a_{jd} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{ni} & \ldots & a_{nd} \end{array}\right].$$

Introduction to lattices

Example

- Rank $n = 3$,
- Dimension $d = 2$,
- The basis is (b_1, b_2) with

$$b_1 = \begin{bmatrix} 1 \\ \sqrt{2} \\ -3 \end{bmatrix}, \quad b_2 = \begin{bmatrix} -2 \\ \frac{\sqrt{3}}{4} \\ -\sqrt{5} \end{bmatrix}.$$

- The lattice $\mathcal{L}$ generated by (b_1, b_2) is the set

$$\mathcal{L} = \left\{v, \quad v = x_1 b_1 + x_2 b_2, \quad (x_1, x_2) \in \mathbb{Z}^2\right\}.$$

Introduction to lattices

Example: Lattice with dimension 2

Exercice

Consider the lattice with basis (b_1, b_2) *where*

$$b_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \; b_2 = \begin{bmatrix} 0.5 \\ 1 \end{bmatrix}.$$

Draw the lattice $\mathcal{L} = \left\{v, \; v = x_1 b_1 + x_2 b_2, \; (x_1, x_2) \in \mathbb{Z}^2\right\}.$

Introduction to lattices

Example: Lattice with dimension 2

$$b_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix},\ b_2 = \begin{bmatrix} 0.5 \\ 1 \end{bmatrix},\ \mathcal{L} = \left\{v,\ v = x_1 b_1 + x_2 b_2,\ (x_1, x_2) \in \mathbb{Z}^2\right\}.$$

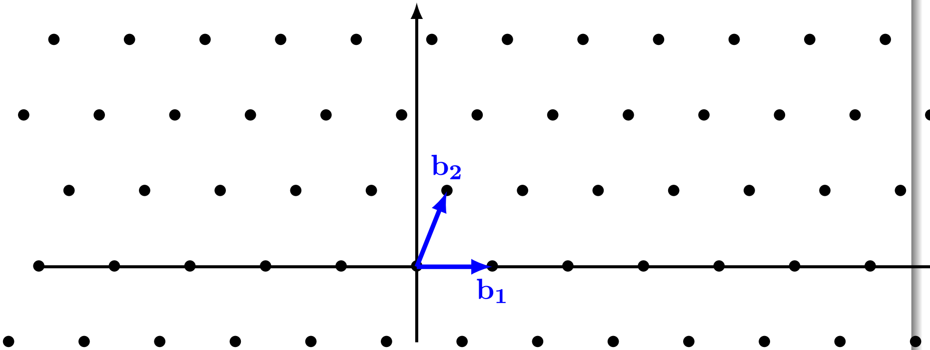
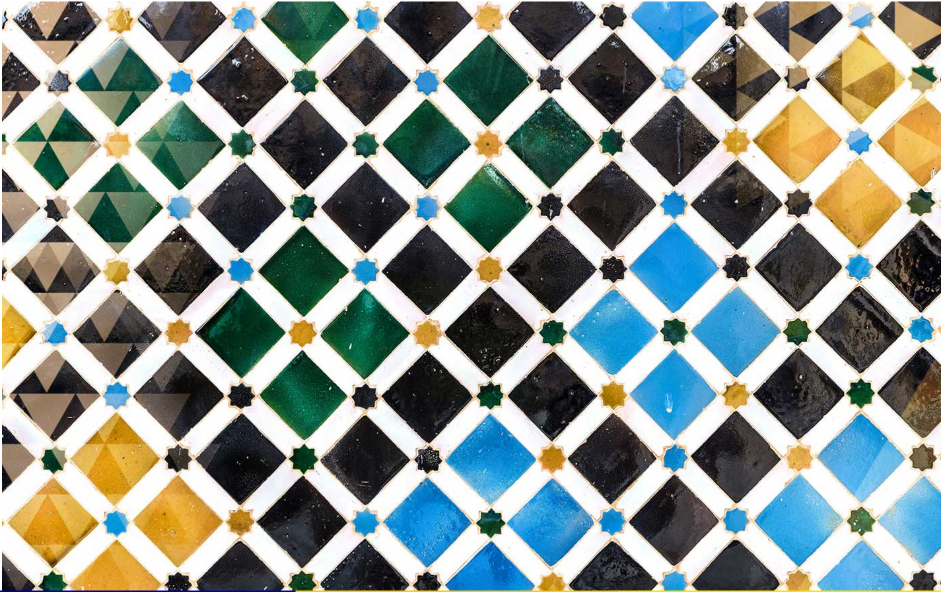


Figure: The lattice with the basis (b_1, b_2)

Introduction to lattices



Introduction to lattices

Proposition

Let $\mathcal{L}$ be a lattice of dimension d and rank n, with a basis $(b_1 \cdots, b_d)$. Then $\mathcal{L}$ can be written as the columns of a $n \times d$ matrix B with real entries.

Exercice

Prove the proposition.

Introduction to lattices

Proposition

Let $\mathcal{L}$ be a lattice of dimension d and rank n, with a basis $(b_1 \cdots, b_d)$. Then $\mathcal{L}$ can be written as the columns of a $n \times d$ matrix B with real entries.

Proof.

Let $(b_1 \cdots, b_d)$ be a basis of $\mathcal{L}$ such that, for $1 \leq i \leq d$, $b_i = \begin{bmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{ni} \end{bmatrix}$.

Let $v \in \mathcal{L}$. Then $v = \sum_{i=1}^{d} x_i b_i$ for $x_i \in \mathbb{Z}$. Hence v can be rewritten as

$$v = x_1 \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{bmatrix} + \ldots + x_d \begin{bmatrix} a_{1d} \\ a_{2d} \\ \vdots \\ a_{nd} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1d} \\ a_{21} & a_{22} & \cdots & a_{2d} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nd} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{bmatrix}.$$

Introduction to lattices

Proposition

Let $\mathcal{L} \subset \mathbb{R}^n$ *be a lattice of dimension* d. *Let* $(b_1 \cdots, b_d)$ *and* $(b'_1 \cdots, b'_d)$ *be two bases of* $\mathcal{L}$. *Then there exists a* $d \times d$ *matrix* U *with entries in* $\mathbb{Z}$ *and* $\det(U) = \pm 1$ *such that*

$$\begin{bmatrix} b'_1 \\ \vdots \\ b'_d \end{bmatrix} = U \begin{bmatrix} b_1 \\ \vdots \\ b_d \end{bmatrix}.$$

Exercice

Prove the proposition.

Introduction to lattices

Proposition

Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice of dimension d. Let $(b_1 \cdots, b_d)$ and $(b'_1 \cdots, b'_d)$ be two bases of $\mathcal{L}$. Then there exists a $d \times d$ matrix U with entries in $\mathbb{Z}$ and $\det(U) = \pm 1$ such that

$$(b'_1, \ldots, b'_d)^t = U(b_1, \ldots, b_d)^t.$$

Proof.

$$\begin{bmatrix} b'_1 \\ \vdots \\ b'_d \end{bmatrix} = \begin{bmatrix} u_{11}b_1 + \ldots + u_{1d}b_d \\ \vdots \\ u_{d1}b_1 + \ldots + u_{dd}b_d \end{bmatrix} = \begin{bmatrix} u_{11} & \cdots & u_{1d} \\ \vdots & \vdots & \vdots \\ u_{d1} & \cdots & u_{dd} \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_d \end{bmatrix} =$$

$U \begin{bmatrix} b_1 \\ \vdots \\ b_d \end{bmatrix}$. Also, $\begin{bmatrix} b_1 \\ \vdots \\ b_d \end{bmatrix} = U' \begin{bmatrix} b'_1 \\ \vdots \\ b'_d \end{bmatrix}$. Then $U'U = I_d$ and $\det(U) = \pm 1$. □

Introduction to lattices

Definition

Let $\mathcal{L}$ be a lattice with a basis $(b_1 \cdots, b_d)$. The volume or determinant of $\mathcal{L}$ is

$$\det(\mathcal{L}) = \sqrt{\det\left(\left(B^T\right)B\right)},$$

where B is the $n \times d$ matrix formed by the columns of the basis vectors.

Exercice

Let $\mathcal{L}$ be the lattice with basis (b_1, b_2) and

$$b_1 = \begin{bmatrix} 1 \\ 3 \\ -2 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}.$$

Compute $\det(\mathcal{L})$.

Introduction to lattices

Example

- Rank $n = 3$,
- Dimension $d = 2$,
- The basis is (b_1, b_2) with $b_1 = \begin{bmatrix} 1 \\ 3 \\ -2 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}$.
- The matrix is $B = \begin{bmatrix} 1 & 2 \\ 3 & 1 \\ -2 & 0 \end{bmatrix}$.
- Then $B^T = \begin{bmatrix} 1 & 3 & -2 \\ 2 & 1 & 0 \end{bmatrix}$ and $\left(B^T\right) B = \begin{bmatrix} 14 & 5 \\ 5 & 5 \end{bmatrix}$
- The volume or determinant of $\mathcal{L}$ is $\det(\mathcal{L}) = \sqrt{\det\left(\left(B^T\right) B\right)} = \sqrt{45}$.

Introduction to lattices

Proposition

Let $\mathcal{L}$ be a full-rank lattice ($n = d$) with a basis $(b_1 \cdots, b_d)$. The volume or determinant of $\mathcal{L}$ is

$$\det(\mathcal{L}) = \sqrt{\det\left(\left(B^T\right)B\right)} = |\det(B)|,$$

where B is the $n \times d$ matrix of formed by the rows of the basis.

Exercice

Prove the proposition.

Introduction to lattices

Proposition

Let $\mathcal{L}$ be a full-rank lattice ($n = d$) with a basis $(b_1 \cdots, b_d)$. The volume or determinant of $\mathcal{L}$ is

$$\det(\mathcal{L}) = \sqrt{\det\left(\left(B^T\right) B\right)} = |\det(B)|,$$

where B is the $n \times d$ matrix of formed by the rows of the basis.

Proof.

We have

$$\det\left(\left(B^T\right) B\right) = \det\left(B^T\right) \det(B) = (\det(B))^2.$$

Hence $\det(\mathcal{L}) = \sqrt{(\det(B))^2} = |\det(B)|$. $\square$

Introduction to lattices

Exercice

Let $\mathcal{L}$ *be the lattice with basis* (b_1, b_2) *and*

$$b_1 = \begin{bmatrix} 1 \\ 3 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

Compute $\det(\mathcal{L})$.

Introduction to lattices

Example

- Rank $n = 2$,
- Dimension $d = 2$,
- The basis is (b_1, b_2) with $b_1 = \begin{bmatrix} 1 \\ 3 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$.
- The matrix is $B = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}$.
- The volume or determinant of $\mathcal{L}$ is

$$\det(\mathcal{L}) = |\det(\mathcal{L})| = |1 - 6| = 5.$$

Introduction to lattices

Proposition

Let $\mathcal{L}$ be a lattice of dimension d. Then the $\det(\mathcal{L})$ is independent of the choice of the basis.

Exercice

Prove the proposition.

Introduction to lattices

Proposition

Let $\mathcal{L}$ be a lattice of dimension d. Then the $\det(\mathcal{L})$ is independent of the choice of the basis.

Proof.

- Let $(b_1 \cdots, b_d)$ be a basis of $\mathcal{L}$. Then $\det(\mathcal{L}) = \sqrt{\det\left(\left(B^T\right)B\right)}$.
- Let $(b'_1 \cdots, b'_d)$ be another basis of $\mathcal{L}$.
- There exists $U \in \mathbb{Z}^{d\times d}$ with $\det(U) = \pm 1$ such that $B' = UB$.
- Then

$$\begin{aligned}\det\left(\left(B'^T\right)B'\right) &= \det\left(\left(B^T U^T\right)UB\right)\\ &= \det\left(U^T\right)\det\left(\left(B^T\right)B\right)\det(U)\\ &= \det\left(\left(B^T\right)B\right).\end{aligned}$$

- Hence $\sqrt{\det\left(\left(B'^T\right)B'\right)} = \sqrt{\det\left(\left(B^T\right)B\right)} = \det(\mathcal{L})$.

$\square$

Introduction to lattices

Definition

Let $\mathcal{L}$ be a lattice with a basis $(b_1 \cdots, b_d)$. The fundamental domain or parallelepipede for $\mathcal{L}$ is the set

$$\mathcal{P}(b_1 \cdots, b_d) = \left\{ \sum_{i=1}^{d} x_i b_i, \mid 0 \leq x_i < 1 \right\}.$$

Proposition

Let $\mathcal{L}$ be a lattice with a basis $(b_1, \ldots, b_d)$. The determinant $\det(\mathcal{L})$ of the lattice is the volume $\mathcal{V}$ of the fundamental domain $\mathcal{P}(b_1, \ldots, b_d)$, that is

$$\det(\mathcal{L}) = \mathcal{V}(\mathcal{P}(b_1, \ldots, b_d)).$$

Introduction to lattices

Lattice with dimension 2

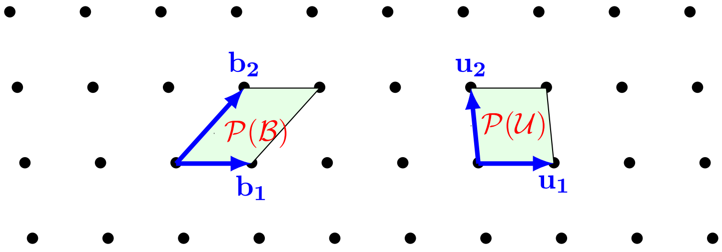


Figure: The fundamental domain for the bases (b_1, b_2) and (u_1, u_2)

Introduction to lattices

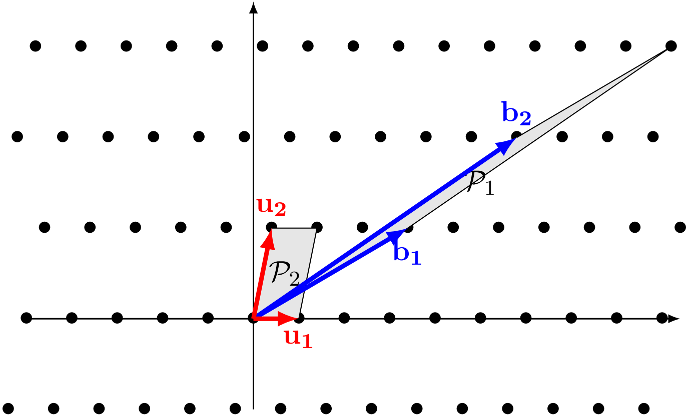


Figure: A lattice with two parallelepipeds and the same area

Introduction to lattices

Proposition

Let $\mathcal{L}$ be a lattice. Then $\mathcal{L}$ has infinitely many bases.

- Let $(b_1 \cdots, b_d)$ and $(b'_1 \cdots, b'_d)$ be two bases of $\mathcal{L}$. Then there exists a $d \times d$ matrix $U \in \mathbb{Z}^{d\times d}$ and $\det(U) = \pm 1$ such that

$$\begin{bmatrix} b'_1 \\ \vdots \\ b'_d \end{bmatrix} = U \begin{bmatrix} b_1 \\ \vdots \\ b_d \end{bmatrix}.$$

- The equation $\det(U) = \pm 1$ has infinitely many solutions in $U \in \mathbb{Z}^{d\times d}$.
- Example: if $d = 2$ and $U = \begin{bmatrix} 3 & 5 \\ y & x \end{bmatrix}$, then $\det(U) = 3x - 5y = 1$ has infinitely many solutions $(x, y) \in \mathbb{Z}^2$.

Introduction to lattices

How to find v?

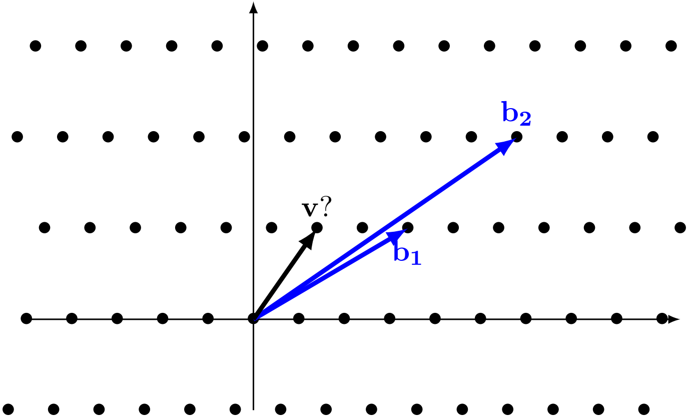


Figure: A lattice with *a bad* basis (b_1, b_2)

Introduction to lattices

How to find v?

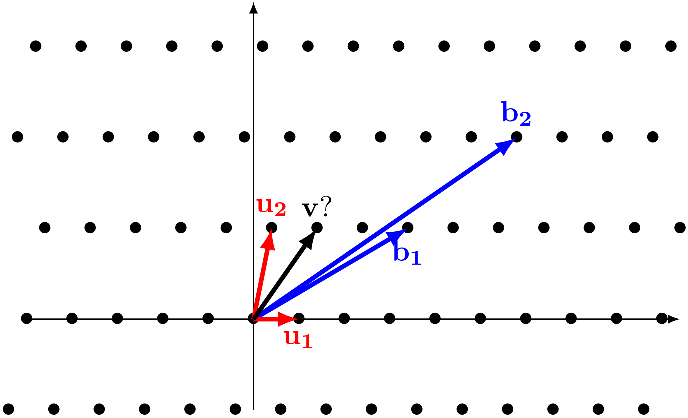


Figure: The same lattice with *a good* basis (u_1, u_2)

Introduction to lattices

A good basis

- In a lattice some bases are better than others.
- A good basis is a basis with
  - Short vectors.
  - Almost orthogonal vectors.

Introduction to lattices

Comparison of bases

- In a lattice some bases are better than others.
- A good basis is a basis with
  - Short vectors.
  - Almost orthogonal vectors.

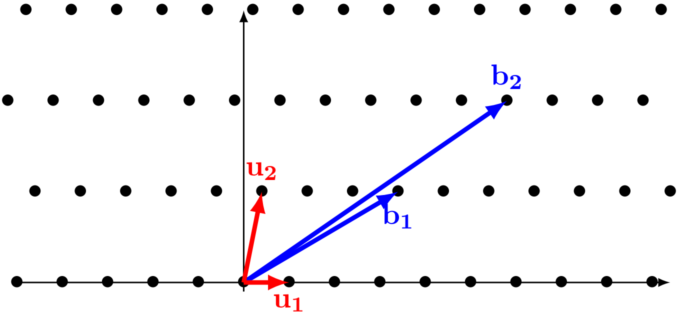


Figure: Comparison of the two bases

Short vectors

Inner product and Euclidean norm

Definition

Let $u = (u_1, \cdots, u_n)$ and $v = (v_1 \cdots, v_n)$ be two vectors of $\mathbb{R}^n$.

1. The inner product of u and v is
$$\langle u, v \rangle = u^T v = \sum_{i=1}^{n} u_i v_i.$$
2. The Euclidean norm of u is
$$\|u\| = (\langle u, u \rangle)^{\frac{1}{2}} = \left(\sum_{i=1}^{n} u_i^2 \right)^{\frac{1}{2}}.$$

Short vectors

Shortest vector

Definition

Let $\mathcal{L}$ be a lattice. The minimal distance λ_1 of $\mathcal{L}$ is the length of the shortest nonzero vector of $\mathcal{L}$:

$$\lambda_1 = \inf\{\|v\| : \ v \in \mathcal{L}\backslash\{0\}\}.$$

Short vectors

The shortest vector

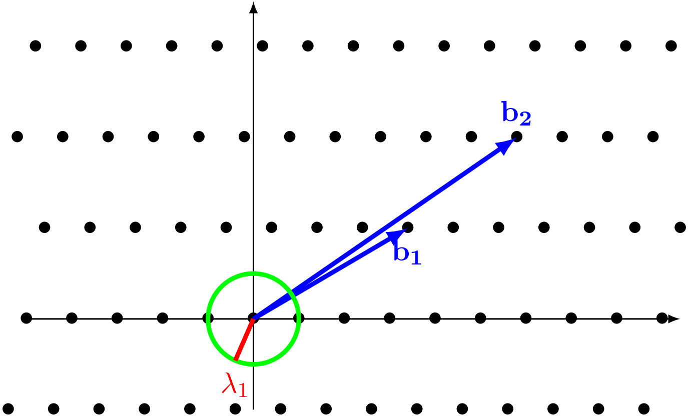


Figure: The shortest vector

Short vectors

Definition (The ith successive minimum)

Let L be a lattice of dimension n. For $i = 1, \dots n$, the ith successive minimum of the lattice is

$$\lambda_i = \min\{\max\{\|v_1\|, \dots, \|v_i\|\} \mid v_1, \dots, v_i \in \mathcal{L} \text{ are linearly independent}\}.$$

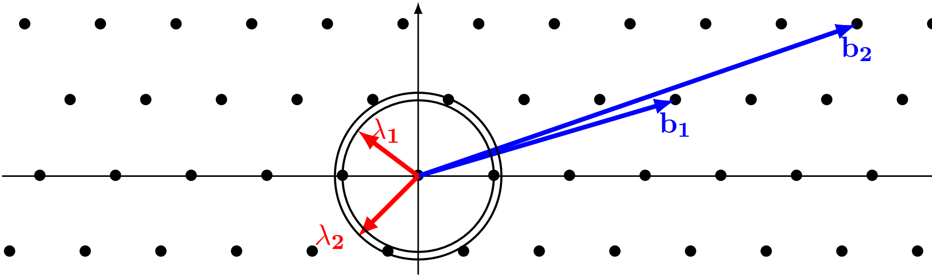


Figure: The first minima λ_1 and the second minima λ_2

Short vectors

Definition (The Shortest Vector Problem (SVP))

Given a basis matrix B for $\mathcal{L}$, compute a non-zero vector $v \in \mathcal{L}$ such that $\|v\|$ is minimal, that is $\|v\| = \lambda_1(\mathcal{L})$.

Short vectors

Theorem (Minkowski's Theorem)

Let $\mathcal{L}$ be a lattice with dimension n. Then there exists a non-zero vector $v \in \mathcal{L}$ satisfying

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

Example

- Let $\mathcal{L}$ be a lattice with a basis (b_1, b_2) with
$$b_1 = \begin{bmatrix} 19239 \\ 2971 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 22961 \\ 3546 \end{bmatrix}.$$
- The determinant is $\det(\mathcal{L}) = 4363$.
- The shortest non-zero vector is $v = 37b_1 - 31b_2 = \begin{bmatrix} 52 \\ 1 \end{bmatrix}$.
- The norm is $\|v\| = \sqrt{2705} \approx 52$.
- Minkowski's bound $\sqrt{n}\,\det(L)^{\frac{1}{n}} \approx 93$.

Closest Vectors

Definition (The Closest Vector Problem (CVP))

Given a basis matrix B for $\mathcal{L}$ and a vector $v \notin \mathcal{L}$, compute a vector $v_0 \in \mathcal{L}$ such that $\|v - v_0\|$ is minimal.

Closest Vectors

The closest vector

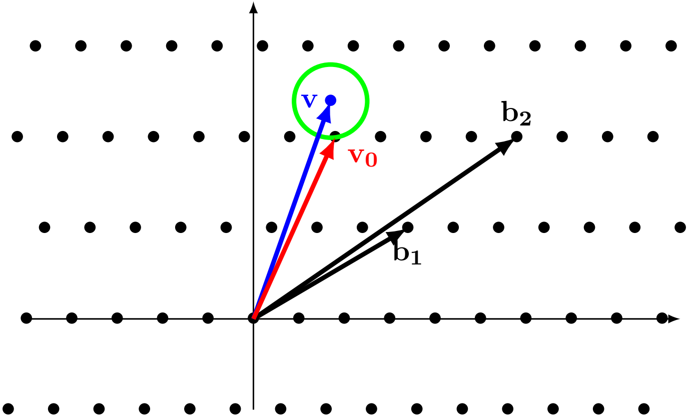


Figure: The closest vector to v is v_0

Lattice problems

Definition

Let $\mathcal{L}$ be a full rank lattice of dimension n in $\mathbb{Z}^n$.

1. **The Shortest Vector Problem (SVP):** $\|v\| = \lambda_1(\mathcal{L})$.
2. **The Closest Vector Problem (CVP):** $\|v - u\|$ is minimal.
3. **The Shortest Independent Vectors Problem (SIVP):** Given a basis matrix B for $\mathcal{L}$, find n linearly independent lattice vectors $v_1, v_2, \ldots, v_n$ such that $\max_i \|v_i\| \leq \lambda_n$, where λ_n is the nth successive minima of $\mathcal{L}$.
4. **The approximate SVP problem (γSVP):** Fix $\gamma > 1$. Given a basis matrix B for $\mathcal{L}$, compute a non-zero vector $v \in \mathcal{L}$ such that $\|v\| \leq \gamma\lambda_1(\mathcal{L})$ where $\lambda_1(\mathcal{L})$ is the minimal Euclidean norm in $\mathcal{L}$.
5. **The approximate CVP problem (γCVP):** Fix $\gamma > 1$. Given a basis matrix B for $\mathcal{L}$ and a vector $v \notin \mathcal{L}$, find a vector $u \in \mathcal{L}$ such that $\|v - u\| \leq \gamma\lambda_1 \mathrm{d}(v, \mathcal{L})$ where $\mathrm{d}(v, \mathcal{L}) = \min_{u\in\mathcal{L}} \|v - u\|$.

Contents

Mauritania

The LLL algorithm

- Invented in 1982 by Lenstra, Lenstra and Lovász.
- Given an arbitrary basis B of a lattice $\mathcal{L}$, LLL finds a "good" basis.
- Polynomial time algorithm.
- Various applications:
  1. Formulae for π, $\log 2$, ...
  2. Implemented in Mathematica, Maple, Magma, Pari/GP, ...
  3. Solving diophantine equations.
  4. Solving SVP and CVP problems in low dimensions.
  5. Cryptanalysis of Knapsack cryptosystems.
  6. Attacks on RSA and NTRU.

Gram-Schmidt orthogonalization method

Theorem

Let V *be a vector space of dimension* n *and* $(b_1 \cdots, b_n)$ *a basis of* V*. Let* $(b_1^* \cdots, b_n^*)$ *be* n *vectors such that*

$$b_1^* = b_1, \quad b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*,$$

where, for $j < i$

$$\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}.$$

Then $(b_1^* \cdots, b_n^*)$ *is an orthogonal basis of* V*.*

Exercice

Prove the theorem.

Gram-Schmidt orthogonalization method

Proof.

- $(b_1^* \cdots, b_n^*)$ is a basis of V

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_{n-1} \\ b_n \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ \mu_{2,1} & 1 & 0 & 0 & \cdots & 0 \\ \mu_{3,1} & \mu_{3,2} & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mu_{n_1,1} & \mu_{n-1,2} & \mu_{n-1,3} & \cdots & 1 & 0 \\ \mu_{n,1} & \mu_{n,2} & \mu_{n,3} & \cdots & \mu_{n,n-1} & 1 \end{bmatrix} \begin{bmatrix} b_1^* \\ b_2^* \\ b_3^* \\ \vdots \\ b_{n-1}^* \\ b_n^* \end{bmatrix}.$$

- Hence $\det(U) = 1$.
- $b_1^* = b_1$ et $b_2^* = b_2 - \mu_{2,1} b_1$, then $\langle b_1^*, b_2^* \rangle = 0$.
- By recursion, $\langle b_k^*, b_i^* \rangle = 0$ for $k \neq i$.

□

Gram-Schmidt orthogonalization method

Proof.

The basis $(b_1^* \cdots, b_n^*)$ is orthogonal.

- Since $b_1^* = b_1$ and $b_2^* = b_2 - \mu_{1,1} b_1^*$, then

$$\begin{aligned}\langle b_1^*, b_2^* \rangle &= \langle b_1, b_2 - \mu_{2,1} b_1 \rangle = \langle b_1, b_2 \rangle - \mu_{2,1} \langle b_1, b_1 \rangle \\ &= \langle b_1, b_2 \rangle - \frac{\langle b_2, b_1 \rangle}{\langle b_1, b_1 \rangle} \langle b_1, b_1 \rangle = 0.\end{aligned}$$

- By recursion, if $(b_1^* \cdots, b_{i-1}^*)$ is orthogonal for $i \geq 3$, then for $1 \leq k \leq i-1$,

$$\begin{aligned}\langle b_k^*, b_i^* \rangle &= \left\langle b_k^*, b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \right\rangle = \langle b_k^*, b_i \rangle - \mu_{i,k} \langle b_k^*, b_k^* \rangle \\ &= \langle b_k^*, b_i \rangle - \frac{\langle b_i, b_k^* \rangle}{\langle b_k^*, b_k^* \rangle} \langle b_k^*, b_k^* \rangle = 0.\end{aligned}$$

Gram-Schmidt orthogonalization method

Gram-Schmidt orthogonalization method: $n = 2$

$$b_1^* = b_1, \quad b_2^* = b_2 - \frac{\langle b_2, b_1\rangle}{\langle b_1, b_1\rangle} b_1,$$

$$\Rightarrow \langle b_1^*, b_2^*\rangle = \langle b_1, b_2\rangle - \frac{\langle b_2, b_1\rangle}{\langle b_1, b_1\rangle}\langle b_1, b_1\rangle = 0.$$

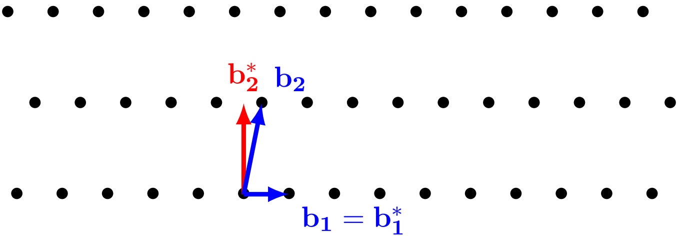


Figure: An orthogonal basis (b_1^*, b_2^*)

Gram-Schmidt orthogonalization method

Gram-Schmidt orthogonalization method: the algorithm

Algorithm 1 : Gram-Schmidt process

Require: A basis $(b_1 \cdots, b_n)$ of a space vector $V \subset \mathbb{R}^n$.
Ensure: An orthogonal basis $(b_1^* \cdots, b_n^*)$ of V.

```
Set b_1^* = b_1.
for i = 1, 2, ··· n, do
    for j = 1, 2, ··· i − 1, do
        Compute μ_{i,j} = ⟨b_i, b_j^*⟩ / ⟨b_j^*, b_j^*⟩.
    end for
    Compute b_i^* = b_i − Σ_{j=1}^{i−1} μ_{i,j} b_j^*.
end for
```

Set $b_1^* = b_1$.
for $i = 1, 2, \cdots n$, **do**
  for $j = 1, 2, \cdots i - 1$, **do**
    Compute $\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$.
  end for
  Compute $b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*$.
end for

Gram-Schmidt orthogonalization method

Exercice

Give the associated orthogonal Gram-Schmidt vectors for :

1. $b_1 = (3, 1)$, $b_2 = (1, 2)$.
2. $b_1 = (3, 2, 5)$, $b_2 = (2, 4, -1)$, $b_3 = (-2, -1, 6)$.

Gram-Schmidt orthogonalization method

Exercice

Give the associated orthogonal Gram-Schmidt vectors for :

1. $b_1 = (3, 1)$, $b_2 = (1, 2)$.
2. $b_1 = (3, 2, 5)$, $b_2 = (2, 4, -1)$, $b_3 = (-2, -1, 6)$.

We get

1. $b_1^* = (3, 1)$, $\mu_{2,1} = \frac{\langle b_2, b_1^* \rangle}{\langle b_1^*, b_1^* \rangle} = \frac{1}{2}$, $b_2^* = b_2 - \mu_{2,1} b_1 = \left(-\frac{1}{2}, \frac{3}{2}\right)$.
2. $$b_1^* = (3, 2, 5),$$
$$\mu_{2,1} = \frac{9}{38}, \quad b_2^* = \left(\frac{49}{38}, \frac{67}{19}, -\frac{83}{38}\right),$$
$$\mu_{3,1} = \frac{11}{19}, \quad \mu_{3,2} = -\frac{730}{717}, \quad b_3^* = \left(-\frac{1738}{717}, \frac{1027}{717}, \frac{632}{717}\right).$$

Gram-Schmidt orthogonalization method

Proposition

Let $B = \{b_1, \ldots, b_n\}$ *be a basis of a lattice* $\mathcal{L}$ *and* $B^* = \{b_1^*, \ldots, b_n^*\}$ *be the associated Gram-Schmidt basis. Then for* $1 \leq i \leq n$,

$$\|b_i^*\| \leq \|b_i\|.$$

Exercice

Prove the Proposition

Gram-Schmidt orthogonalization method

Proposition

Let $B = \{b_1, \ldots, b_n\}$ be a basis of a lattice $\mathcal{L}$ and $B^* = \{b_1^*, \ldots, b_n^*\}$ be the associated Gram-Schmidt basis. Then for $1 \leq i \leq n$,

$$\|b_i^*\| \leq \|b_i\|.$$

Proof.

- For $i = 1$, $\|b_1^*\| = \|b_1\|$
- For $2 \leq i \leq n$, $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{i,j} b_j^*$, Then

$$\|b_i\|^2 = \|b_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 \|b_j^*\|^2 \geq \|b_i^*\|^2.$$

$\square$

Gram-Schmidt orthogonalization method

Proposition

Let $B = \{b_1, \ldots, b_n\}$ be a basis of a lattice $\mathcal{L}$ and $B^* = \{b_1^*, \ldots, b_n^*\}$ be the associated Gram-Schmidt basis. Then for $1 \leq i \leq n$,

$$\|b_i^*\| \leq \|b_i\|.$$

Gram-Schmidt orthogonalization method: the determinant

Corollary (Hadamard)

Let $B = \{b_1, \ldots, b_n\}$ be a basis of a lattice $\mathcal{L}$ and let $B^* = \{b_1^*, \ldots, b_n^*\}$ be the associated Gram-Schmidt basis. Then

$$\det(\mathcal{L}) = \prod_{i=1}^{n} \|b_i^*\| \leq \prod_{i=1}^{n} \|b_i\|.$$

The LLL algorithm

Definition

Let $\mathcal{L}$ be a lattice. A basis $(b_1 \cdots, b_n)$ of $\mathcal{L}$ is LLL-reduced if the orthogonal Gram-Schmidt basis $(b_1^* \cdots, b_n^*)$ satisfies

$$\begin{aligned} |\mu_{i,j}| &\leq \frac{1}{2}, \quad \text{pour} \quad 1 \leq j < i \leq n, && (1)\\ \frac{3}{4}\|b_{i-1}^*\|^2 &\leq \|b_i^* + \mu_{i,i-1}b_{i-1}^*\|^2, \quad \text{pour} \quad 1 < i \leq n, && (2)\end{aligned}$$

where, for $j < i$

$$\mu_{i,j} = \frac{\langle b_i, b_j^*\rangle}{\langle b_j^*, b_j^*\rangle}.$$

Condition (2) can be transformed into the inequality

$$\left(\frac{3}{4} - \mu_{i,i-1}^2\right)\|b_{i-1}^*\|^2 \leq \|b_i^*\|^2.$$

The LLL algorithm

LLL-reduced basis: dimension 2

- $\langle b_2, b_1^* \rangle = \|b_1\| \|b_2\| \cos(b_1, b_2)$.
- $|\mu_{2,1}| = \left| \frac{\langle b_2, b_1^* \rangle}{\langle b_1^*, b_1^* \rangle} \right| = \frac{\|b_1\| \|b_2\| |\cos(b_1, b_2)|}{\|b_1\|^2}$.
- $|\mu_{2,1}| \leq \frac{1}{2}$ means $|\cos(b_1, b_2)|$ is small and $b_1 \approx\perp b_2$.
- $\left(\frac{3}{4} - |\mu_{2,1}|^2\right) \|b_1^*\|^2 \leq \|b_2^*\|^2$ means b_2^* can be short.

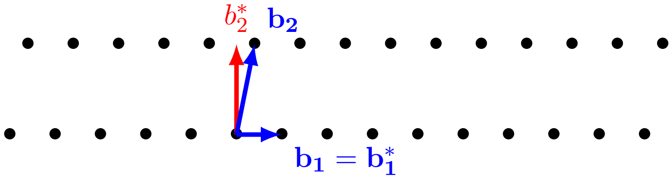


Figure: An 2-dimension reduced basis

The LLL algorithm

LLL-reduced basis: properties

Let $(b_1 \cdots, b_n)$ be an LLL-reduced basis and $(b_1^*, \cdots, b_n^*)$ be the Gram-Schmidt orthogonal associated basis.

1. $\|b_j^*\|^2 \leq 2^{i-j}\|b_i^*\|^2$ for $1 \leq j \leq i \leq n$.
2. $\prod_{i=1}^n \|b_i\| \leq 2^{\frac{n(n-1)}{4}} \det(L)$.
3. $\|b_j\| \leq 2^{\frac{i-1}{2}}\|b_i^*\|$ for $1 \leq j \leq i \leq n$.
4. $\|b_1\| \leq 2^{\frac{n-1}{4}}(\det(L))^{\frac{1}{n}}$.
5. $\|b_j\| \leq 2^{\frac{n(n-1)}{4(n-j+1)}}(\det L)^{\frac{1}{n-j+1}}$.
6. For any nonzero vector $v \in L$, $\|b_1\| \leq 2^{\frac{n-1}{2}}\|v\|$.

The LLL algorithm

Comparison

- The LLL algorithm: $\|b_1\| \leq 2^{\frac{n-1}{4}} \det(L)^{\frac{1}{n}}$.
- Minkowski: $\|v\| \leq \sqrt{n}\det(L)^{\frac{1}{n}}$.

Theorem

Let $(b_1, \cdots, b_n)$ *be a basis of a lattice* $\mathcal{L}$ *of dimension* n. *Define* $B = \max_i \|b_i\|$. *The LLL algorithm computes an LLL-reduced basis with running time*

$$\mathcal{O}\left(n^4 \log^3 B\right).$$

The LLL algorithm

Example

- Let $\mathcal{L}$ be a lattice with a basis (u_1, u_2) with
$$u_1 = \begin{bmatrix} 12104590255 \\ 16053445447 \end{bmatrix}, \quad u_2 = \begin{bmatrix} 509666982522 \\ 675934577519 \end{bmatrix}.$$
- The determinant is $\det(\mathcal{L}) = 11$.
- $\boxed{\text{The LLL algorithm: } \|b_1\| \leq 2^{\frac{1}{4}} \det(L)^{\frac{1}{2}} \approx 3.9.}$
- The LLL outputs the basis $(b_1, b_2$ with $b_1 = \begin{bmatrix} 2 \\ 3 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 1 \\ -4 \end{bmatrix}$.
- The smallest norm is $\|b_1\| = \sqrt{13} \approx 3.6$.

The LLL algorithm

Example

Find $(x_1, x_2, x_3) \in \mathbb{Z}^3$ such that $F(x_1, x_2, x_3) \neq 0$ is minimal where

$$
\begin{aligned}
&F(x_1, x_2, x_3)\\
&= (23795990x_1 + 2789321x_2 + 6722230x_3)^2\\
&+ (10618674239468197x_1 + 4045209235436167x_2 + 3033906925524537x_3)^2\\
&+ (175016190714715827x_1 + 66672834559179425x_2 + 50004625917609416x_3)^2.
\end{aligned}
$$

- Consider the vector

$$
v = \begin{bmatrix} 23795990x_1 + 2789321x_2 + 6722230x_3 \\ 10618674239468197x_1 + 4045209235436167x_2 + 3033906925524537x_3 \\ 175016190714715827x_1 + 66672834559179425x_2 + 50004625917609416x_3 \end{bmatrix}.
$$

The LLL algorithm

Example

Find $(x_1, x_2, x_3) \in \mathbb{Z}^3$ such that $F(x_1, x_2, x_3) \neq 0$ is minimal where

$$\begin{aligned}
&F(x_1, x_2, x_3)\\
&= (23795990x_1 + 2789321x_2 + 6722230x_3)^2\\
&+ (10618674239468197x_1 + 4045209235436167x_2 + 3033906925524537x_3)^2\\
&+ (17501619071471582 7x_1 + 6667283455917942 5x_2 + 5000462591760941 6x_3)^2.
\end{aligned}$$

- Then $v = x_1u_1 + x_2u_2 + x_3u_3$ with $u_1 = \begin{bmatrix} 23795990 \\ 2789321 \\ 6722230 \end{bmatrix}$,

$$u_2 = \begin{bmatrix} 10618674239468197 \\ 4045209235436167 \\ 3033906925524537 \end{bmatrix}, \quad u_3 = \begin{bmatrix} 17501619071471582 7 \\ 6667283455917942 5 \\ 5000462591760941 6 \end{bmatrix}.$$

The LLL algorithm

Example

Find $(x_1, x_2, x_3) \in \mathbb{Z}^3$ such that $F(x_1, x_2, x_3) \neq 0$ is minimal where

$$\begin{aligned} &F(x_1, x_2, x_3) \\ &= (23795990x_1 + 2789321x_2 + 6722230x_3)^2 \\ &+ (10618674239468197x_1 + 4045209235436167x_2 + 3033906925524537x_3)^2 \\ &+ (17501619071471 5827x_1 + 6667283455917942 5x_2 + 5000462591760941 6x_3)^2. \end{aligned}$$

- Apply the LLL algorithm to get

$$\begin{bmatrix} b_1 \to & -23 & 11 & 12 \\ b_2 \to & -2 & -21 & -16 \\ b_3 \to & 20 & -19 & 27 \end{bmatrix}$$

The LLL algorithm

Example

Find $(x_1, x_2, x_3) \in \mathbb{Z}^3$ such that $F(x_1, x_2, x_3) \neq 0$ is minimal where

$$
\begin{aligned}
&F(x_1, x_2, x_3)\\
&= (23795990x_1 + 2789321x_2 + 6722230x_3)^2\\
&+ (1061867423946819 7x_1 + 4045209235436167x_2 + 3033906925524537x_3)^2\\
&+ (17501619071471582 7x_1 + 66672834559179425x_2 + 50004625917609416x_3)^2.
\end{aligned}
$$

- Solve the equation

$$
\begin{bmatrix} 23795990x_1 + 2789321x_2 + 6722230x_3 \\ 10618674239468197x_1 + 4045209235436167x_2 + 3033906925524537x_3 \\ 175016190714715827x_1 + 66672834559179425x_2 + 50004625917609416x_3 \end{bmatrix} = \begin{bmatrix} -23 \\ 11 \\ 12 \end{bmatrix}.
$$

- We get

$$(x_1, x_2, x_3) = (-7618906333339779895 9, -3309671943642864303, 2710746175966032920 55).$$

- The minimal is then $F(x_1, x_2, x_3) = (-23)^2 + 11^2 + 12^2 = 794.$

The LLL algorithm

Algorithm 2 : The LLL algorithm

Require: A basis $(u_1, \cdots, u_n)$

Ensure: An LLL reduced basis $(b_1, \cdots, b_n)$

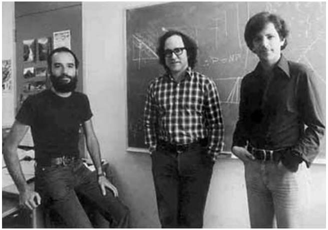
For $i = 1, \ldots, n$, $b_i = u_i$.
$k = 2$
while $k \leq n$ **do**
    for $j = 1, \ldots, k-1$ **do**
        $\mu_{k,j} = \frac{\langle b_k, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$, $b_k = b_k - \lfloor \mu_{k,j} \rceil b_k^*$.
    end for
    if $\|b_k^*\|^2 \geq \left(\frac{3}{4} - \mu_{k,k-1}^2\right) \|b_{k-1}^*\|^2$ **then**
        $k = k + 1$.
    else
        Swap b_{k-1} and b_k, $k = \max(k-1, 2)$.
    end if
end while
Return $(b_1, \cdots, b_n)$.

Contents

Mauritania

The RSA Cryptosystem

- Invented in 1978 by Rivest, Shamir and Adleman.



- The most widely used asymmetric cryptosystem.
- The security of RSA is based on two hard problems:
  1. The integer factorization problem.
  2. The RSA Problem (the eth modular root).

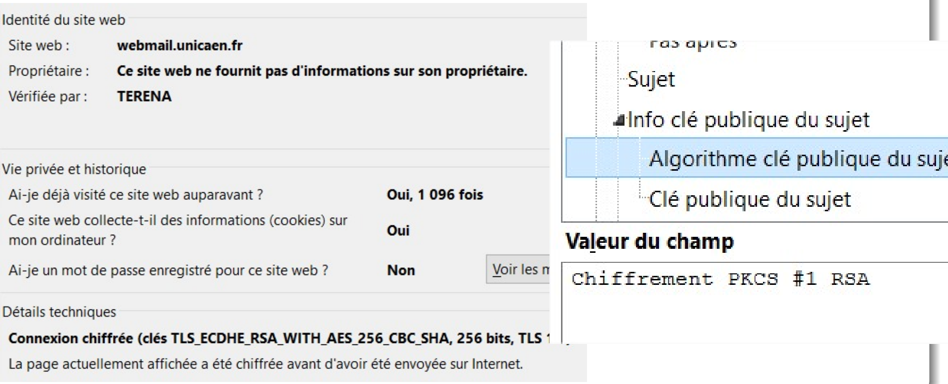
The RSA Cryptosystem

The most widely used cryptosystem

1. Encryption and digital signature.
2. Implemented in most Web servers and browsers.
3. Securing e-commerce and e-mail.
4. Authenticity of electronic documents.
5. Most commercially available security products.

Cryptography and the Internet

Cryptographic Protocols



Cryptography and the Internet

Cryptographic Protocols

Info clé publique du sujet

Algorithme clé publique du sujet

Clé publique du sujet

Valeur du champ

```
Module (2048 bits) :
bd bc 7e 50 5f b7 ac d0 12 68 c7 c6 1d fc 6c
32 e8 d3 eb 97 39 f8 24 b6 ed 87 cd f5 0d 59
f1 e1 18 e6 56 48 bc 81 74 26 ce 2a d7 d4 a7
a6 fa 7f a8 bd d2 78 fe f0 7c 04 4b e3 73 22
c3 1d 18 4c d0 2a 57 0d bc d2 34 84 f0 d8 87
cd 43 cb 94 f6 c5 b9 34 56 5c 0f e3 35 9e 5a
90 c2 0d 7a 6e fa 9e d4 02 54 ee b3 8b bf a3
22 c7 01 ba 99 a9 b3 da b2 00 0d d5 68 22 9f 4b
```

Algorithme clé publique du sujet

Clé publique du sujet

Extensions

Identificateur de la clé d'autorité de certification

Valeur du champ

```
9a e8 c4 c2 d2 31 f1 c5 2b d6 5c a7 c2 4d
17 0e cb 10 60 5d 10 1f 1a 86 4c 92 57 31
fe 2c eb a4 f9 13 ee b4 a1 93 cf 28 5f 86
30 e7 ff e6 1a 6a 2a 08 a2 56 62 49 ae 42
ed 59 53 41 36 8d 10 9d 78 10 d1 7a 70 ae

Exposant (24 bits) :
65537
```

Coppersmith's method

Polynomial equation

Given a multivariate polynomial f and a modulus N, find a solution $(x_1, \ldots, x_n)$ of the equation

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{N}.$$

Principles of Coppersmith's method

1. f is a polynomial with small roots.
2. Use f to build ω polynomials sharing the roots.
3. Use the new polynomials to build a lattice $\mathcal{L}$ with a basis B.
4. Apply the LLL algorithm to reduce the basis B.
5. Solve the polynomials of the reduced basis using Howgrave-Graham's Theorem and resultant or Gröbner Basis techniques.

Coppersmith's method

The attack of Boneh and Durfee

- Start with $ed - k(p-1)(q-1) = 1$.
- Transform to $k(N - p - q + 1) + 1 \equiv 0 \pmod{e}$.
- Consider $f(x, y) = x(N + y) + 1 \equiv 0 \pmod{e}$.
- Then $\boxed{f(k, -p - q - 1) \equiv 0 \pmod{e}.}$
- For m and t positive integers, $0 \le k \le m$, define the polynomials

$$\begin{aligned} g_{k,i_1}(x, y) &= x^{i_1 - k} f(x, y)^k e^{m-k}, \quad & k \le i_1 \le m, \\ h_{k,i_2}(x, y) &= y^{i_2 - k} f(x, y)^k e^{m-k}, \quad & k + 1 \le i_2 \le k + t. \end{aligned}$$

Coppersmith's method

Exercice

1. *Show that* $\boxed{g_{k,i_1}(k, -p-q-1) \equiv 0 \pmod{e^m}.}$
2. *Show that* $\boxed{h_{k,i_2}(k, -p-q-1) \equiv 0 \pmod{e^m}.}$
3. *Let* $m = 2$ *and* $t = 1$. *For* $0 \leq k \leq m$, *compute* $g_{k,i_1}(x, y)$ *and* $h_{k,i_2}(x, y)$.

Coppersmith's method

Exercice

- *We have* $\boxed{f(k,-p-q-1) \equiv 0 \pmod{e}.}$
- *Then*

$$\begin{aligned} g_{k,i_1}(k,-p-q-1) &= k^{i_1-k} f(k,-p-q-1)^k e^{m-k} \\ &= k^{i_1-k} a e^k e^{m-k} = b e^m. \end{aligned}$$

Hence $g_{k,i_1}(k,-p-q-1) \equiv 0 \pmod{e^m}$.

- *Also,*

$$\begin{aligned} h_{k,i_2}(k,-p-q-1) &= (-p-q-1)^{i_2-k} f(k,-p-q-1)^k e^{m-k} \\ &= (-p-q-1)^{i_2-k} a' e^k e^{m-k} = b' e^m. \end{aligned}$$

Hence $h_{k,i_2}(k,-p-q-1) \equiv 0 \pmod{e^m}$.

Coppersmith's method

Exercice

Let $m = 2$ and $t = 1$. Compute $g_{k,i_1}(x,y) = x^{i_1-k} f(x,y)^k e^{m-k}$ for $0 \le k \le m$ and $k \le i_1 \le m$.

We have

$$
\begin{aligned}
&g_{0,0}(x,y) = e^2, \quad g_{0,1}(x,y) = e^2 x, \quad g_{0,2}(x,y) = e^2 x^2,\\
&g_{1,1}(x,y) = (xy + Nx + 1)e = e + Nex + exy,\\
&g_{1,2}(x,y) = x(xy + Nx + 1)e = e + Nex^2 + ex^2 y,\\
&g_{2,2}(x,y) = (xy + Nx + 1)^2 = 1 + 2Nx + Nx^2 + 2xy + 2Nx^2 y + x^2 y^2.
\end{aligned}
$$

Coppersmith's method

Exercice

Let $m = 2$ *and* $t = 1$*. Compute* $h_{k,i_2}(x,y) = y^{i_2-k} f(x,y)^k e^{m-k}$ *for* $0 \le k \le m$ *and* $k+1 \le i_2 \le k+t$*.*

We have

$$\begin{aligned} h_{0,1}(x,y) &= ye, \\ h_{1,2}(x,y) &= y(xy+Nx+1)e = Nexy + ey + exy^2, \\ h_{2,3}(x,y) &= y(xy+Nx+1)^2 \\ &= y + 2Nxy + Nx^2y + 2xy^2 + 2Nx^2y^2 + x^2y^3. \end{aligned}$$

Coppersmith's method

Exercice

Let $m = 2$ and $t = 1$. For $k = 0, \dots, m$, collect the monomials of $g_{k,i_1}(x, y)$ and $h_{k,i_2}(x, y)$.

k	g, h	1	x	x^2	y	xy	x^2y	xy^2	x^2y^2	x^2y^3
$k=0$	$g_{0,0}$	$\boxed{e^2}$	0	0	0	0	0	0	0	0
$k=0$	$g_{0,1}$	0	$\boxed{e^2}$	0	0	0	0	0	0	0
$k=0$	$g_{0,2}$	0	0	$\boxed{e^2}$	0	0	0	0	0	0
$k=0$	$h_{0,1}$	0	0	0	$\boxed{e}$	0	0	0	0	0
$k=1$	$g_{1,1}$	e	Ne	0	0	$\boxed{e}$	0	0	0	0
$k=1$	$g_{1,2}$	e	0	Ne	0	0	$\boxed{e}$	0	0	0
$k=1$	$h_{1,2}$	0	0	0	e	Ne	0	$\boxed{e}$	0	0
$k=2$	$g_{2,2}$	1	$2N$	N	0	2	$2N$	0	$\boxed{1}$	0
$k=2$	$h_{2,3}$	0	0	0	1	$2N$	N	2	$2N$	$\boxed{1}$

Coppersmith's method

Proposition

Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then

$$\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}, \quad p + q < 3\sqrt{N}.$$

Exercice

Prove the proposition.

Coppersmith's method

Proposition

Let $N = pq$ be an RSA modulus and $e < \phi(N) = (p-1)(q-1)$ be a public exponent such that $ed - k\phi(N) = 1$. Then $k < d$.

Exercice

Prove the proposition.

Coppersmith's method

The attack of Boneh and Durfee

- In the equation $ed - k\phi(N) = 1$, suppose that $\boxed{d < N^\delta}$.
- Let $X = N^\delta$ and $Y = 3N^{\frac{1}{2}}$.
- Then $k < d < X$ and $p + q - 1 < 3N^{\frac{1}{2}} = Y$.
- Form a lattice $\mathcal{L}$ with the coefficients of the polynomials $g_{k,i_1}(Xx, Yy)$ and $h_{k,i_2}(Xx, Yy)$.

Coppersmith's method

The attack of Boneh and Durfee

Form a lattice $\mathcal{L}$ with the coefficients of the polynomials $g_{k,i_1}(Xx, Yy)$ and $h_{k,i_2}(Xx, Yy)$.

$g,\ h$	1	x	x^2	y	xy	x^2y	xy^2	x^2y^2	x^2y^3
$g_{0,0}$	e^2	0	0	0	0	0	0	0	0
$g_{0,1}$	0	Xe^2	0	0	0	0	0	0	0
$g_{0,2}$	0	0	X^2e^2	0	0	0	0	0	0
$h_{0,1}$	0	0	0	Ye	0	0	0	0	0
$g_{1,1}$	$*$	$*$	0	0	XYe	0	0	0	0
$g_{1,2}$	$*$	0	$*$	0	0	X^2Ye	0	0	0
$h_{1,2}$	0	0	0	$*$	$*$	0	XY^2e	0	0
$g_{2,2}$	$*$	$*$	$*$	0	$*$	$*$	0	X^2Y^2	0
$h_{2,3}$	0	0	0	$*$	$*$	$*$	$*$	$*$	X^2Y^3

Coppersmith's method

The attack of Boneh and Durfee

- Consider $f(x, y) = x(N + y) + 1 \equiv 0 \pmod{e}$.
- Then $\boxed{f(k, -p - q - 1) \equiv 0 \pmod{e}.}$
- For m and t positive integers, $0 \leq k \leq m$, define the polynomials

$$g_{k,i_1}(x, y) = x^{i_1 - k} f(x, y)^k e^{m-k}, \quad 0 \leq k \leq m, \quad k \leq i_1 \leq m,$$
$$h_{k,i_2}(x, y) = y^{i_2 - k} f(x, y)^k e^{m-k}, \quad 0 \leq k \leq m, \quad k + 1 \leq i_2 \leq k + t.$$

- Form a lattice $\mathcal{L}$ with the coefficients of the polynomials $g_{k,i_1}(Xx, Yy)$ and $h_{k,i_2}(Xx, Yy)$.

Exercice

- *Prove that any polynomial* $P(Xx, Yy) \in \mathcal{L}$ *satisfies* $P(k, -p - q + 1) \equiv 0 \pmod{e^m}$.
- *Give the general form for* $\det(\mathcal{L})$.

Coppersmith's method

The attack of Boneh and Durfee

- For m and t positive integers, form a lattice $\mathcal{L}$ with the coefficients of the polynomials $g_{k,i_1}(Xx, Yy)$ and $h_{k,i_2}(Xx, Yy)$ with

$$\begin{aligned} g_{k,i_1}(Xx, Yy) &= (Xx)^{i_1-k} f(Xx, Yy)^k e^{m-k}, \\ & \qquad 0 \leq k \leq m, \quad k \leq i_1 \leq m, \\ h_{k,i_2}(Xx, Yy) &= (Yy)^{i_2-k} f(Xx, Yy)^k e^{m-k}, \\ & \qquad 0 \leq k \leq m, \quad k+1 \leq i_2 \leq k+t. \end{aligned}$$

- Since $g(k, -p-q+1) \equiv 0 \pmod{e^m}$, $h(k, -p-q+1) \equiv 0 \pmod{e^m}$ and $P(x, y) = ag(x, y) + bh(x, y)$ with $a, b \in \mathbb{Z}$, then $h(k, -p-q+1) \equiv 0 \pmod{e^m}$.
- The determinant of the lattice is

$$\boxed{\det(\mathcal{L}) = e^{n_e} X^{n_X} Y^{n_Y}.}$$

Coppersmith's method

The attack of Boneh and Durfee

- For m and t positive integers, form a lattice $\mathcal{L}$ with the coefficients of the polynomials $g_{k,i_1}(Xx, Yy)$ and $h_{k,i_2}(Xx, Yy)$ with

$$\begin{aligned} g_{k,i_1}(Xx,Yy) &= (Xx)^{i_1-k} f(Xx,Yy)^k e^{m-k}, \\ & \qquad 0 \le k \le m, \quad k \le i_1 \le m, \\ h_{k,i_2}(Xx,Yy) &= (Yy)^{i_2-k} f(Xx,Yy)^k e^{m-k}, \\ & \qquad 0 \le k \le m, \quad k+1 \le i_2 \le k+t. \end{aligned}$$

- The determinant of the lattice is

$$\boxed{\det(\mathcal{L}) = e^{n_e} X^{n_X} Y^{n_Y}.}$$

Exercice

Compute the dimension ω of $\mathcal{L}$ and the exponents n_e, n_X and n_Y.

Coppersmith's method

The attack of Boneh and Durfee

$$
\begin{aligned}
g_{k,i_1}(Xx,Yy) &= (Xx)^{i_1-k} f(Xx,Yy)^k e^{m-k}, \\
&\qquad 0 \le k \le m, \quad k \le i_1 \le m, \\
h_{k,i_2}(Xx,Yy) &= (Yy)^{i_2-k} f(Xx,Yy)^k e^{m-k}, \\
&\qquad 0 \le k \le m, \quad k+1 \le i_2 \le k+t.
\end{aligned}
$$

- The dimension of $\mathcal{L}$ is

$$
\omega = \sum_{k=0}^{m} \sum_{i_1=k}^{m} 1 + \sum_{k=0}^{m} \sum_{i_2=k+1}^{k+t} 1 = \frac{(m+1)(m+2t+2)}{2}.
$$

Coppersmith's method

The attack of Boneh and Durfee

$$\begin{aligned} g_{k,i_1}(Xx,Yy) &= (Xx)^{i_1-k} f(Xx,Yy)^k e^{m-k}, \\ & \qquad 0 \le k \le m, \quad k \le i_1 \le m, \\ h_{k,i_2}(Xx,Yy) &= (Yy)^{i_2-k} f(Xx,Yy)^k e^{m-k}, \\ & \qquad 0 \le k \le m, \quad k+1 \le i_2 \le k+t. \end{aligned}$$

- The exponent of e is $m-k$. Then

$$n_e = \sum_{k=0}^{m}\sum_{i_1=k}^{m}(m-k) + \sum_{k=0}^{m}\sum_{i_2=k+1}^{k+t}(m-k) = \frac{m(m+1)(2m+3t+4)}{6}.$$

Coppersmith's method

The attack of Boneh and Durfee

$$
\begin{aligned}
g_{k,i_1}(Xx, Yy) &= (Xx)^{i_1-k} f(Xx, Yy)^k e^{m-k}, \\
&\qquad 0 \le k \le m, \quad k \le i_1 \le m, \\
h_{k,i_2}(Xx, Yy) &= (Yy)^{i_2-k} f(Xx, Yy)^k e^{m-k}, \\
&\qquad 0 \le k \le m, \quad k+1 \le i_2 \le k+t.
\end{aligned}
$$

- The exponents of X are i_1 and k. Then

$$
n_X = \sum_{k=0}^{m} \sum_{i_1=k}^{m} i_1 + \sum_{k=0}^{m} \sum_{i_2=k+1}^{k+t} k = \frac{m(m+1)(2m+3t+4)}{6}.
$$

Coppersmith's method

The attack of Boneh and Durfee

$$
\begin{aligned}
g_{k,i_1}(Xx,Yy) &= (Xx)^{i_1-k} f(Xx,Yy)^k e^{m-k},\\
&\qquad 0 \le k \le m, \quad k \le i_1 \le m,\\
h_{k,i_2}(Xx,Yy) &= (Yy)^{i_2-k} f(Xx,Yy)^k e^{m-k},\\
&\qquad 0 \le k \le m, \quad k+1 \le i_2 \le k+t.
\end{aligned}
$$

- The exponent of Y are k and i_2. Then

$$
n_Y = \sum_{k=0}^{m}\sum_{i_1=k}^{m} k + \sum_{k=0}^{m}\sum_{i_2=k+1}^{k+t} i_2 = \frac{(m+1)(m^2+3tm+2m+3t^2+3t)}{6}.
$$

Coppersmith's method

The attack of Boneh and Durfee

- $\omega = \frac{(m+1)(m+2t+2)}{2}$.
- $n_e = \frac{m(m+1)(2m+3t+4)}{6}$.
- $n_X = \frac{m(m+1)(2m+3t+4)}{6}$.
- $n_Y = \frac{(m+1)(m^2+3tm+2m+3t^2+3t)}{6}$.

Exercice

Let $t = \tau m$. *Find the dominant part of* ω, n_e, n_X *and* n_Y.

Coppersmith's method

The attack of Boneh and Durfee

- Put $t = m\tau$. Then

$$\omega' = \left(\frac{1}{2} + \tau\right) m^2 + o(m^2),$$

$$n_e' = \left(\frac{1}{3} + \frac{1}{2}\tau\right) m^3 + o(m^3),$$

$$n_X' = \left(\frac{1}{3} + \frac{1}{2}\tau\right) m^3 + o(m^3),$$

$$n_Y' = \left(\frac{1}{6} + \frac{1}{2}\tau + \frac{1}{2}\tau^2\right) m^3 + o(m^3).$$

Coppersmith's method

The attack of Boneh and Durfee

- Apply the LLL algorithm to the lattice $\mathcal{L}$.
- It outputs a reduced basis $P_1(Xx, Yy), P_2(Xx, Yy), \ldots, P_\omega(Xx, Yy)$. (LLL properties p. 54)
- The first polynomials satisfy

$$\|P_1(Xx, Yy)\|\|\| \leq 2^{\frac{n-1}{4}} \det(\mathcal{L})^{\frac{1}{n}},$$

$$\|P_2(Xx, Yy)\| \leq 2^{\frac{n}{4}} \det(\mathcal{L})^{\frac{1}{n-1}}.$$

Definition

Let $P(x, y) = \sum_i \sum_j a_{i,j} x^i y^j \in \mathbb{Z}[x, y]$. Then the Euclidean norm of $P(x, y)$ is

$$\boxed{\|P(x, y)\| = \sqrt{\sum_i \sum_j a_{i,j}^2}.}$$

Coppersmith's method

The attack of Boneh and Durfee

The polynomials $P_1(Xx, Yy)\|$ and $\|P_2(Xx, Yy)$ satisfy

- $\|P_1(Xx, Yy)\|, \|P_2(Xx, Yy)\| \leq 2^{\frac{n}{4}} \det(\mathcal{L})^{\frac{1}{n-1}}$.
- $P_1(k, -p-q+1) \equiv 0 \pmod{e^m}$, $P_2(k, -p-q+1) \equiv 0 \pmod{e^m}$.

Theorem (Howgrave-Graham)

Let $P(x, y) \in \mathbb{Z}[x, y]$ be a polynomial with at most ω monomials. Suppose that

1. $P(x_0, y_0) \equiv 0 \pmod{e^m}$,
2. $|x_0| < X, |y_0| < Y$,
3. $\|P(Xx, Yx)\| < \frac{e^m}{\sqrt{\omega}}$.

Then $P(x_0, y_0) = 0$ holds over the integers.

Exercice

Prove the theorem.

Coppersmith's method

Howgrave-Graham

- We have

$$|P(x_0,y_0)| = \left|\sum_{i,j} a_{i,j}x_0^i y_0^j\right| \le \sum_{i,j}\left|a_{i,j}x_0^i y_0^j\right| < \sum_{i,j}\left|a_{i,j}X^iY^j\right|.$$

- The Cauchy-Schwarz inequality asserts that for $\alpha, \beta \in \mathbb{R}$, we have

$$\left(\sum_{i,j}\alpha_{i,j}\beta_{i,j}\right)^2 \le \left(\sum_{i,j}\alpha_{i,j}^2\right)\left(\sum_{i,j}\beta_{i,j}^2\right).$$

- Using this, we get $\left(\sum_{i,j}\left|a_{i,j}X^iY^j\right|\right)^2 \le \left(\sum_{i,j}1^2\right)\left(\sum_{i,j}\left(a_{i,j}X^iY^j\right)^2\right) =$ $\omega\sum_{i,j}\left(a_{i,j}X^iY^j\right)^2 = \omega\|P(Xx,Yx)\|^2$.

Coppersmith's method

Howgrave-Graham

- We have $|P(x_0,y_0)| < \sqrt{\omega}\|P(Xx,Yx)\|$.
- If $\|P(Xx,Yx)\| < \frac{e^m}{\sqrt{\omega}}$, then $|P(x_0,y_0)| < \sqrt{\omega}\|P(Xx,Yy)\| < e^m$.
- If $P\left(x_0,y_0\right) \equiv 0 \pmod{e^m}$, then $P\left(x_0,y_0\right) = 0$.

Coppersmith's method

Proposition

Let $P_1(x,y), P_2(x,y) \in \mathbb{Z}[x,y]$ *be two polynomial with at most* ω *monomials. Suppose that*

1. $P_1(k, -p-q+1) \equiv 0 \pmod{e^m}$ *and* $P_2(k, -p-q+1) \equiv 0 \pmod{e^m}$,
2. $|k| < X, |-p-q+1| < Y$,
3. $\|P_1(Xx, Yx)\| < \frac{e^m}{\sqrt{\omega}}$ *and* $\|P_2(Xx, Yx)\| < \frac{e^m}{\sqrt{\omega}}$.

Then $(k, -p-q+1)$ *is a solution of the system* $\begin{cases} P_1(x_0, y_0) = 0 \\ P_2(x_0, y_0) = 0. \end{cases}$

The attack of Boneh and Durfee

The first polynomials of the lattice $\mathcal{L}$ satisfy condition (1) and (2) and

$$\|P_1(Xx, Yy)\|, \|P_2(Xx, Yy)\| \leq 2^{\frac{\omega}{4}} \det(\mathcal{L})^{\frac{1}{\omega-1}}.$$

Coppersmith's method

The attack of Boneh and Durfee

- Set $2^{\frac{\omega}{4}}\det(\mathcal{L})^{\frac{1}{\omega-1}} < \frac{e^m}{\sqrt{\omega}}$.
- Then
$$\det(\mathcal{L} < \frac{1}{\left(\sqrt{\omega}2^{\frac{\omega}{4}}\right)^{\omega-1}}e^{m(\omega-1)} < e^{m\omega}.$$
- Since $\det(\mathcal{L}) \approx e^{n'_e}X^{n'_X}Y^{n'_Y}$ (p. 87) with $X = N^{\delta}$, $Y = 3N^{\frac{1}{2}}$ and $e \approx N$, then
$$N^{n'_e}N^{n'_X\delta}N^{\frac{1}{2}n'_Y} < e^{m\omega} \approx N^{m\omega'}$$
- Taking logarithms, we get $n'_e + n'_X\delta + \frac{1}{2}n'_Y < m\omega'$. Then

$$\left(\frac{1}{3}+\frac{1}{2}\tau\right)m^3 + \left(\frac{1}{3}+\frac{1}{2}\tau\right)m^3\delta + \frac{1}{2}\left(\frac{1}{6}+\frac{1}{2}\tau+\frac{1}{2}\tau^2\right)m^3 < \left(\frac{1}{2}+\tau\right)m^3$$

Coppersmith's method

The attack of Boneh and Durfee

We have

$$\left(\frac{1}{3}+\frac{1}{2}\tau\right)m^3+\left(\frac{1}{3}+\frac{1}{2}\tau\right)m^3\delta+\frac{1}{2}\left(\frac{1}{6}+\frac{1}{2}\tau+\frac{1}{2}\tau^2\right)m^3 < \left(\frac{1}{2}+\tau\right)m^3$$

Exercice

Rearrange the inequality in terms of τ.

Coppersmith's method

The attack of Boneh and Durfee

We have

$$\left(\frac{1}{3}+\frac{1}{2}\tau\right)m^3+\left(\frac{1}{3}+\frac{1}{2}\tau\right)m^3\delta+\frac{1}{2}\left(\frac{1}{6}+\frac{1}{2}\tau+\frac{1}{2}\tau^2\right)m^3 < \left(\frac{1}{2}+\tau\right)m^3$$

Rearranging, we get

$$\frac{1}{6}\left(-\frac{1}{2}+2\delta\right)+\frac{1}{2}\left(-\frac{1}{2}+\delta\right)\tau+\frac{1}{4}\tau^2<0.$$

Exercice

1. *Find the optimal value* τ_0.
2. *Plug* τ_0 *and find a new inequality.*
3. *Solve for* δ.

Coppersmith's method

The attack of Boneh and Durfee

Rearranging, we get

$$\frac{1}{6}\left(-\frac{1}{2}+2\delta\right)+\frac{1}{2}\left(-\frac{1}{2}+\delta\right)\tau+\frac{1}{4}\tau^2<0.$$

1. This is optimized for $\tau_0=\frac{1}{2}-\delta$.
2. Plugging τ_0, we get $-12\delta^2+28\delta-7<0$.
3. Solving for δ, we get

$$\delta<\frac{7}{6}+\frac{\sqrt{7}}{3}\approx 2.048,\quad \delta<\frac{7}{6}-\frac{\sqrt{7}}{3}\approx 0.284.$$

4. Hence $\delta<\frac{7}{6}-\frac{\sqrt{7}}{3}\approx 0.284$.

Coppersmith's method

The attack of Boneh and Durfee

- Suppose that $ed - k(N - p - q + 1) = 1$ with $d < N^{\delta}$ with $\delta < \frac{7}{6} - \frac{\sqrt{7}}{3} \approx 0.284$.
- Find $P_1(x, y)$ and $P_2(x, y)$ such that

$$\|P_1(Xx, Yy)\|, \|P_2(Xx, Yy)\| \leq 2^{\frac{\omega}{4}} \det(\mathcal{L})^{\frac{1}{\omega-1}}$$

- Solve $P_1(x, y) = 0$ and $P_2(x, y) = 0$ over $\mathbb{Z}^2$ using resultants or Gröbner basis techniques to get $x_0 = k$ and $y_0 = -p - q + 1$.
- Then $d = \frac{k(N-p-q+1)+1}{e}$.
- Using $y_0 = -p - q + 1$ and $N = pq$, we can find p and q.

Exercice

Prove the last assertion.

Contents

Mauritania

NTRU

NTRU

- Invented by Hoffstein, Pipher et Silverman in 1996.
- Security based on the Shortest Vector Problem (SVP).
- Various versions between 1996 and 2001.

Definition

The Shortest Vector Problem (SVP): Given a basis matrix B for $\mathcal{L}$, compute a non-zero vector $v \in \mathcal{L}$ such that $\|v\|$ is minimal, that is $\|v\| = \lambda_1(\mathcal{L})$.

NTRU: Ring of Convolution $\Pi = \mathbb{Z}[X]/(X^N - 1)$

Polynomials

$f = \sum_{i=0}^{N-1} f_i X^i, \qquad g = \sum_{i=0}^{N-1} g_i X^i,$

Sum

$f + g = (f_0 + g_0, f_1 + g_1, \cdots, f_{N-1} + g_{N-1}).$

Product

$f * g = h = (h_0, h_1, \cdots, h_{N-1})$ with

$$\boxed{h_k = \sum_{i+j \equiv k \pmod N} f_i g_j.}$$

NTRU: Ring of Convolution $\Pi = \mathbb{Z}[X]/(X^N - 1)$

Polynomials

$f = \sum_{i=0}^{N-1} f_i X^i, \qquad g = \sum_{i=0}^{N-1} g_i X^i,$

Sum

$f + g = (f_0 + g_0, f_1 + g_1, \cdots, f_{N-1} + g_{N-1}).$

Product

$f * g = h = (h_0, h_1, \cdots, h_{N-1})$ with

$$\boxed{h_k = \sum_{i+j \equiv k \pmod{N}} f_i g_j.}$$

NTRU: Ring of Convolution $\Pi = \mathbb{Z}[X]/(X^N - 1)$

Polynomials

$f = \sum_{i=0}^{N-1} f_i X^i, \qquad g = \sum_{i=0}^{N-1} g_i X^i,$

Sum

$f + g = (f_0 + g_0, f_1 + g_1, \cdots, f_{N-1} + g_{N-1}).$

Product

$f * g = h = (h_0, h_1, \cdots, h_{N-1})$ with

$$\boxed{h_k = \sum_{i+j \equiv k \pmod{N}} f_i g_j.}$$

NTRU: Ring of Convolution $\Pi = \mathbb{Z}[X]/(X^N - 1)$

Convolution

$$\underbrace{f = (f_0, f_1, \cdots, f_{N-1}), \qquad g = (g_0, g_1, \cdots, g_{N-1})}_{f * g = h = (h_0, h_1, \cdots, h_{N-1})}.$$

	1	X	$\cdots$	X^k	$\cdots$	X^{N-1}
	$f_0 g_0$	$f_0 g_1$	$\cdots$	$f_0 g_k$	$\cdots$	$f_0 g_{N-1}$
$+$	$f_1 g_{N-1}$	$f_1 g_0$	$\cdots$	$f_1 g_{k-1}$	$\cdots$	$f_1 g_{N-2}$
$+$	$f_2 g_{N-2}$	$f_2 g_{N-1}$	$\cdots$	$f_2 g_{k-2}$	$\cdots$	$f_2 g_{N-3}$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\cdots$	$\vdots$	$\vdots$
$+$	$f_{N-2} g_2$	$f_{N-2} g_3$	$\cdots$	$f_{N-2} g_{k+2}$	$\cdots$	$f_{N-2} g_1$
$+$	$f_{N-1} g_1$	$f_{N-1} g_2$	$\cdots$	$f_{N-1} g_{k+1}$	$\cdots$	$f_{N-1} g_0$
$h =$	h_0	h_1	$\cdots$	h_k	$\cdots$	h_{N-1}

NTRU Parameters

- $N =$ a prime number (e.g. $N = 167,\ 251,\ 347,\ 503$).
- $q =$ a large modulus (e.g. $q = 128,\ 256$).
- $p =$ a small modulus (e.g. $p = 3$).

NTRU Algorithms

Key Generation:

- Randomly choose two private polynomials f and g.
- Compute the inverse of f modulo q: $f * f_q = 1 \pmod q$.
- Compute the inverse of f modulo p: $f * f_p = 1 \pmod p$.
- Compute the public key $h = f_q * g \pmod q$.

NTRU Algorithms

Encryption:

- m is a plaintext in the form of a polynomial mod q.
- Randomly choose a private polynomial r.
- Compute the encrypted message $e = m + pr * h \pmod{q}$.

Decryption:

- Compute $a = f * e = f * (m + pr * h) = f * m + pr * g \pmod{q}$.
- Compute $a * f_p = (f * m + pr * g) * f_p = m \pmod{p}$.

NTRU Algorithms

Encryption:

- m is a plaintext in the form of a polynomial mod q.
- Randomly choose a private polynomial r.
- Compute the encrypted message $e = m + pr * h \pmod q$.

Decryption:

- Compute $a = f * e = f * (m + pr * h) = f * m + pr * g \pmod q$.
- Compute $a * f_p = (f * m + pr * g) * f_p = m \pmod p$.

NTRU Algorithms

Encryption:

- m is a plaintext in the form of a polynomial mod q.
- Randomly choose a private polynomial r.
- Compute the encrypted message $e = m + pr * h \pmod{q}$.

Decryption:

- Compute $a = f * e = f * (m + pr * h) = f * m + pr * g \pmod{q}$.
- Compute $a * f_p = (f * m + pr * g) * f_p = m \pmod{p}$.

NTRU

Correctness of decryption

We have

$$\begin{aligned} a &\equiv f * e \pmod q \\ a &\equiv f * (p * r * h + m) \pmod q \\ a &\equiv f * r * (p * g * f_q) + f * m \pmod q \\ a &\equiv p * r * g * f * f_q + f * m \pmod q \\ a &\equiv p * r * g + f * m \pmod q. \end{aligned}$$

If $p * r * g + f * m \in \left[-\frac{q}{2}, \frac{q}{2}\right]$, then

$$m \equiv a * f_p \mod p.$$

MAPLE p. 24

NTRU

Example

Key generation

- Public parameters $N = 13$, $p = 3$, $q = 8$.
- Private keys $f = X^{12} + X^{11} + X^{10} + X^9 + X^8 + X^7 + 1$, $g = X^{12} + X^5 - X^4 + X^3 - X^2 + X - 1$.
- $f * f_p \equiv 1 \pmod p$ with $f_p = 2X^{12}+2X^{11}+2X^{10}+2X^9+2X^8+2X^7+2X^5+2X^4+2X^3+2X^2+2X$.
- $f * f_q \equiv 1 \pmod q$ with $f_q = X^{12}+X^{11}+X^{10}+X^9+X^8+X^7+2X^6+X^5+X^4+X^3+X^2+X+2$.
- The public key is $h \equiv g * f_q \pmod q = 2X^{12} + 2X^{11} + 2X^9 + 2X^7 + 3X^5 + 2X^3 + 2X$.

NTRU

Example

Encryption

- Message $m = X^{10} + X^8 + X^7 + X^4 + X^3 + 1$.
- Random error $r = X^{12} + X^{11} + X^8 + X^7 + 1$.
- The ciphertext $e = \equiv p * r * h + m \pmod q \equiv 5X^{12}+2X^{11}+3X^{10}+2X^9+5X^8+3X^7+2X^6+5X^5+6X^4+4X^3+2X$.

NTRU

Example

Decryption

- $$\begin{aligned} a &\equiv f * e \pmod{q} \\ &\equiv 6X^{12}+3X^{11}+6X^{10}+2X^{9}+3X^{8}+4X^{7} \\ &\quad +6X^{6}+6X^{5}+4X^{4}+7X^{3}+X^{2}+6X+3. \end{aligned}$$

- $$\begin{aligned} m &\equiv f_p * a \pmod{p} \\ &\equiv X^{10}+X^{8}+X^{7}+X^{4}+X^{3}+1, \end{aligned}$$

Application of LLL to NTRU

Contents

Mauritania

GGH

GGH

- Invented by Goldreich, Goldwasser and Halevi in 1996.
- Security based on the Closest Vector Problem (CVP).
- Brocken by Nguyen in 1999.

Definition (The Closest Vector Problem (CVP))

Given a basis matrix B for $\mathcal{L}$ and a vector $v \notin \mathcal{L}$, compute a vector $v_0 \in \mathcal{L}$ such that $\|v - v_0\|$ is minimal.

GGH

Key generation

Algorithm 3 : GGH key generation

Require: A lattice $\mathcal{L}$ of dimension n.

Ensure: A public key B and a private key A.

1: Find a "good basis" A of $\mathcal{L}$.
2: Find a "bad basis" B of $\mathcal{L}$.
3: Publish B as the public key.
4: Keep A as the secret key.

GGH

Encryption

Algorithm 4 : GGH encryption

Require: A lattice $\mathcal{L}$, a parameter $\rho > 0$, a public key B and a plaintext $m \in \mathbb{Z}^n$.

Ensure: A ciphertext c.

1: Compute $v = mB \in \mathcal{L}$.

2: Choose a small vector $e \in [-\rho, \rho]^n$.

3: The ciphertext is $c = v + e$.

GGH

Encryption

Algorithm 5 : GGH decryption

Require: A lattice $\mathcal{L}$, a private key A and a ciphertext c.

Ensure: A plaintext $m \in \mathbb{Z}^n$.

1: Use A to compute $w = cA^{-1} \notin \mathcal{L}$.
2: Use Babai's algorithm to find the closest vector $v \in \mathcal{L}$ to w.
3: Compute $m = (vA)B^{-1}$.

MAPLE p. 20

GGH

Example

Key generation

- The private key A is $A = \begin{bmatrix} 12 & 12 & 19 \\ -1 & -15 & 24 \\ 66 & -24 & -23 \end{bmatrix}$
- The public key B is

$$B = \begin{bmatrix} 829379706506153221 & 669655507050961029 & 1561586631160012960 \\ -756084947558284333 & -610476422212147995 & -1423583985441960558 \\ 1196833256327636 & 966344402656182 & 2253440840184453 \end{bmatrix}$$

GGH

Example

Encryption

- The message is $m = [51, -27, 97]$.
- $v = mB =$ $[44455887216084962654, 35894452606629461698, 83703178711351846467]$
- The error term is $e = [5, 2, 4]$.
- The encrypted message is $c = mB + e =$ $[44455887216084962659, 35894452606629461600, 83703178711351846471]$

GGH

Example

Decryption

- The encrypted message is $c = mB + e =$ $[44455887216084962659, 35894452606629461600, 83703178711351846471]$
- Compute $w = cA^{-1} =$ $[\frac{1818501358582736124881333}{49050}, \frac{30532067579135138513 4}{545}, \frac{3914924010743286852 79}{49050}]$
- Use Babai's algorithm to find $v = \lfloor w \rceil =$ $[3707444156131979867, 56022142347036951 4, 798149645411475 4]$
- Compute $m = (vA)B^{-1} = [51, -27, 97]$.

GGH

Correctness of GGH

- $B = UA$ for some $U \in \mathbb{Z}^{n\times n}$ with $\det(U) = \pm 1$.
- The encrypted message is $c = mB + e = mUA + e$.
- $w = cA^{-1} = (mUA + e)A^{-1} = mU + eA^{-1}$, where eA^{-1} is "small".
- Use Babai's algorithm to find $v = \lfloor w \rceil = mU$, if $|eA^{-1}| < \frac{1}{2}$.
- $(vA)B^{-1} = (mUA)B^{-1} = (mB)B^{-1} = m$.

Hard Problem: CVP

- The encrypted message is $c = mB + e$.
- The Attack: Find mB as the closest vector to c.
- The security is based on the hardness of CVP.
- Solved by Nguyen when the error term e is small enouph.

Contents

Mauritania

Learning With Errors

LWE

- Invented by O. Regev in 2005.
- Security based on the GapSVP problem.
- Provable Security.

Definition

The GapSVP problem: Let $\mathcal{L}$ be a lattice with a basis B. Let $\lambda_1(\mathcal{L})$ be the length of the shortest nonzero vector of $\mathcal{L}$. Let $\gamma > 0$ and $r > 0$. Decide whether $\lambda_1(\mathcal{L}) < r$ or $\lambda_1(\mathcal{L}) > \gamma r$.

Learning With Errors

Example

- Easy: solve the system

$$\begin{bmatrix} 17 & 42 & -127 \\ 24 & 3 & 71 \\ -7 & -23 & 45 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -3265 \\ 246 \\ 1202 \end{bmatrix}$$

- Harder: solve the system

$$\underbrace{\begin{bmatrix} 117 & 422 & -127 \\ 214 & 23 & 71 \\ -17 & -223 & 45 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}}_{S} \underbrace{\begin{matrix} + \\ + \end{matrix}} \underbrace{\begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix}}_{E} \underbrace{\begin{matrix} = \\ = \end{matrix}} \underbrace{\begin{bmatrix} -4718 \\ 4177 \\ 2485 \end{bmatrix}}_{P}$$

- $AS + E = P$: LWE equation over $\mathbb{Z}$.

Learning With Errors

Example

- Hard: solve the system

$$\begin{bmatrix} 17 & 42 & 127 \\ 24 & 3 & 71 \\ 7 & 23 & 45 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 116 & \pmod{503} \\ 158 & \pmod{503} \\ 271 & \pmod{503} \end{bmatrix}$$

- Much harder: solve the system

$$\underbrace{\begin{bmatrix} 117 & 422 & 127 \\ 214 & 23 & 71 \\ 17 & 223 & 45 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}}_{S} \underbrace{+}_{+} \underbrace{\begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix}}_{E} \underbrace{=}_{=} \underbrace{\begin{bmatrix} 144 & \pmod{503} \\ 229 & \pmod{503} \\ 503 & \pmod{503} \end{bmatrix}}_{P}$$

- $AS + E = P$: LWE equation over $\mathbb{Z}_{503}$.

Learning With Errors

LWE Key Generation

Algorithm 6 : LWE Key Generation

Require: Integers n, m, l, q.
Ensure: A private key S and a public key (A, P).

1: Choose $S \in \mathbb{Z}_q^{n\times l}$ at random.
2: Choose $A \in \mathbb{Z}_q^{m\times n}$ at random.
3: Choose $E \in \mathbb{Z}_q^{m\times l}$ according to $\chi(E) = e^{-\pi\|E\|^2/r^2}$ for some $r > 0$.
4: Compute $P = AS + E \pmod{q}$. Hence $P \in \mathbb{Z}_q^{m\times l}$.
5: The private key is S.
6: The public key is (A, P).

Learning With Errors

LWE: Encryption

Algorithm 7 : LWE Encryption

Require: Integers n, m, l, t, r, q, a public key (A, P) and a plaintext $M \in \mathbb{Z}_t^{l\times 1}$.

Ensure: A ciphertext (u, c).

1: Choose $a \in [-r, r]^{m\times 1}$ at random.

2: Compute $u = A^T a \pmod{q} \in \mathbb{Z}_q^{n\times 1}$.

3: Compute $c = P^T a + \left[\frac{Mq}{t}\right] \pmod{q} \in \mathbb{Z}_q^{l\times 1}$.

4: The ciphertext is (u, c).

Learning With Errors

LWE: Decryption

Algorithm 8 : LWE Decryption

Require: Integers n, m, l, t, r, q, a private key S and a ciphertext (u, c).

Ensure: A plaintext M.

1: Compute $v = c - S^T u$ and $M = \left[\frac{tv}{q}\right]$.

Learning With Errors

Correctness of decryption

We have

$$\begin{aligned} v &= c - S^T u \\ &= (AS+E)^T a - S^T A^T a + \left[\frac{Mq}{t}\right] \\ &= E^T a + \left[\frac{Mq}{t}\right]. \end{aligned}$$

Hence

$$\left[\frac{tv}{q}\right] = \left[\frac{tE^T a}{q} + \frac{t}{q}\left[\frac{Mq}{t}\right]\right].$$

With suitable parameters, the term $\frac{tE^T a}{q}$ is negligible and $\frac{t}{q}\left[\frac{Mq}{t}\right] = M$.

Consequently $\left[\frac{tv}{q}\right] = M$.

LWE

Hard Problem

Equations

- The public equation $P = AS + E \pmod{q}$.
- The public ciphertext $c = P^T a + \left[\frac{Mq}{t}\right] \pmod{q}$.
- Can be reduced to the approximate-SVP and GapSVP.

q-ary lattices

Let $A \in \mathbb{Z}_q^{n\times l}$ for some integers q, n, l.

- The q-ary lattice:

$$\Lambda_q(A) = \left\{ y \in \mathbb{Z}^l : \quad y \equiv A^T s \pmod{q} \quad \text{for some} \quad s \in \mathbb{Z}^n \right\}.$$

- The orthogonal q-ary lattice:

$$\Lambda_q^{\perp}(A) = \left\{ y \in \mathbb{Z}^l : \quad Ay \equiv 0 \pmod{q} \right\}.$$

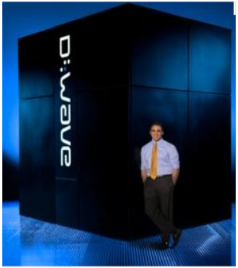
Contents

Mauritania

Conclusion

Lattice cryptography

- Can be used to build cryptographic schemes (GGH, NTRU, LWE,...).
- Can be used to build fully homomorphic encryption, Digital signatures, identity based encryption IBE, hash functions.
- Many hard problems (SVP, CVP, ...).
- Fast implementation.
- Resistance to quantum computers and NSA..



Merci

Thank you

شكرًا