Modern Public Key Cryptography

Lattice Cryptography

Lena Heimberger
based on slides by Lukas Helminger

June 1, 2022

Why Lattice-Based Cryptography?

- Conjectured security against quantum attacks:

  3/4 (PKE) resp. 2/3 (Signature) finalists of NIST PQ-Crypto standardization are lattice-based.

- Novel Constructions:
  - Fully Homomorphic Encryption
  - Attribute-Based Encryption

Outline

Lattices: Definition and Properties

- Fundamental Domain
- Volume
- Computational Problems

Short Integer Solution Problem

- Definition and Properties
- Hardness
- Cryptographic Applications

Literature

The slides are based on the following sources

- **An Introduction to Mathematical Cryptography**, Hoffstein, Jeffrey, Pipher, Jill, Silverman, J.H.
- **A Decade of Lattice Cryptography**, Chris Peikert
- **Talk: The Short Integer Solutions Problem and Cryptographic Applications** by Daniele Micciancio (Lattice Workshop Berkeley)

Many graphics are based on graphics from Maria Eichlseder.

Lattices: Definition and Properties

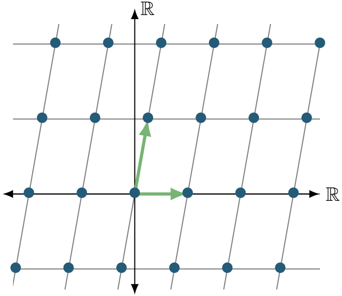
Lattice: Example

Let $v_1, \ldots, v_n \in \mathbb{R}^n$ be a set of linearly independent vectors. The lattice generated by $v_1, \ldots, v_n$ is the set of linear combinations of $v_1, \ldots, v_n$ with coefficients in $\mathbb{Z}$,

$$L = \{a_1 v_1 + \cdots + a_n v_n \ : \ a_1, \ldots, a_n \in \mathbb{Z}\}.$$

Example:

$$\boldsymbol{v}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \boldsymbol{v}_2 = \begin{pmatrix} 1/4 \\ \sqrt{2} \end{pmatrix}$$



Lattices

Definition (Lattice)

An n-dimensional lattice L is any subset of $\mathbb{R}^n$ that is both:

- an additive subgroup
- discrete

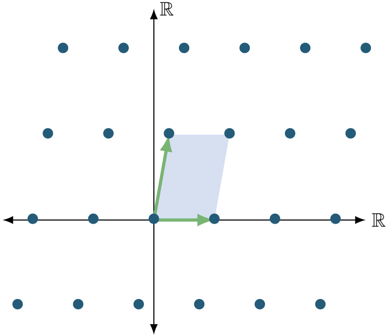
A basis for L is any set of independent vectors that generates L.

Fundamental Domains

Definition (Fundamental Domain)

Let L be a lattice of dimension n and let $v_1, \ldots, v_n$ be a basis for L. The fundamental domain is the set

$$F = [0,1)v_1 + \cdots + [0,1)v_n.$$



Volumes

Definition (Volume)

Let L be a lattice of dimension n and let F be a fundamental domain of L. Then the n-dimensional volume of F is called the volume of L (or sometimes the determinant of L).

Example: Let L be generated by the vectors

$$v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 1/4 \\ \sqrt{2} \end{pmatrix}.$$

we write $L = \mathcal{L}(v_1, v_2)$. First, compute Gram matrix:

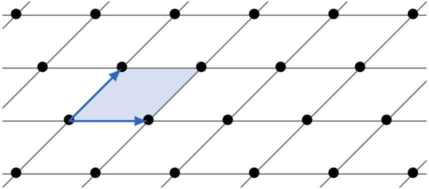
$$G = \begin{pmatrix} 1 & 0 \\ \frac{1}{4} & \sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} 1 & \frac{1}{4} \\ 0 & \sqrt{2} \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{4} \\ \frac{1}{4} & \frac{33}{16} \end{pmatrix}$$

Therefore,

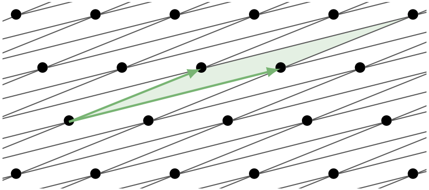
$$\mathrm{vol}(L) = \sqrt{\det G} = \sqrt{2}$$

Same Lattice?

$$\boldsymbol{v}_1 = \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \boldsymbol{v}_2 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$$



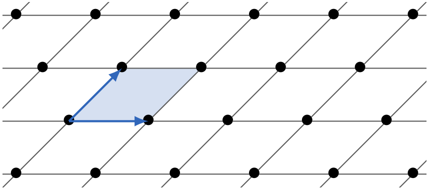
$$\boldsymbol{v}'_1 = \begin{pmatrix} 8 \\ 2 \end{pmatrix}, \boldsymbol{v}'_2 = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$$



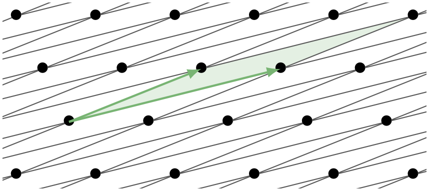
Task: Compute the volumes V resp. V' of the fundamental domains corresponding to $\mathcal{L}(v_1, v_2)$ respectively $\mathcal{L}(v'_1, v'_2)$.

Same Lattice?

$$\boldsymbol{v}_1 = \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \boldsymbol{v}_2 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$$



$$\boldsymbol{v}_1' = \begin{pmatrix} 8 \\ 2 \end{pmatrix}, \boldsymbol{v}_2' = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$$



Proposition

Every fundamental domain for a given lattice L has the same volume.

Minimum Distance

Definition (Minimum Distance)

The minimum distance of a lattice L is the length of a shortest nonzero lattice vector, i.e.,

$$\lambda_1(L) := \min_{v \in L \setminus \{0\}} \|v\|.$$

More generally, the *i*th minimum $\lambda_i(L)$ is defined as the minimum of $\max_{1 \le j \le i} \|v_j\|$ over all i linearly independent lattice vectors $v_1, \ldots, v_i \in L$.

Clearly $\lambda_1(L) \le \cdots \le \lambda_n(L)$.

$$L = \mathcal{L}\left(\begin{pmatrix} 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \end{pmatrix}\right)$$

$$\Rightarrow \lambda_1(L) = \sqrt{8}$$

Computational Problems

- **Shortest Vector Problem (SVP):** Find a shortest nonzero vector $v \in L$, i.e. $\|v\| = \lambda_1(L)$.
- **Approximate Shortest Vector Problem (** SVP_γ **):** Let $\gamma \geq 1$ be a approximation factor. Given a basis B of an n-dimensional lattice L, find a nonzero vector $v \in L$ s.t.

$$\|v\| \leq \gamma(n) \cdot \lambda_1(L).$$

- **Approximate Shortest Independent Vectors Problem (** $SIVP_\gamma$ **):** Given a basis B of an n-dimensional lattice L, find set $\{s_1, \ldots, s_n\} \subset L$ of n linearly independent vectors s.t.

$$\|s_i\| \leq \gamma(n) \cdot \lambda_n(L) \quad \text{for all } i.$$

Summary

- Lattices are "discrete vector spaces".
- Basis of the same lattice can be quite different (from a computational point of view).
- $\lambda_1(L)$ = length of shortest nonzero lattice vector.
- SVP$_\gamma$: Find somewhat short vector.

Short Integer Solution Problem

Short Integer Solution (SIS)

Definition (SIS, Ajtai's function)

Given m uniformly random vectors $a_i \in \mathbb{Z}_q^n$, forming the columns of a matrix $A \in \mathbb{Z}_q^{n \times m}$, find a nonzero integer vector $z \in \mathbb{Z}^m$ of norm $\|z\| \leq \beta$ such that

$$Az = 0 \in \mathbb{Z}_q^n.$$

$f_A(z) := Az \mod q$ is called Ajtai's function, i.e., we are interested in short vectors of the kernel of f_A.

Example: $q = 10, z \in \{0, 1\}^m$

$$\begin{bmatrix} 1 & 4 & 5 & 9 & 3 & 0 & 2 \\ 4 & 2 & 8 & 6 & 2 & 4 & 3 \\ 7 & 5 & 5 & 4 & 7 & 8 & 0 \\ 2 & 7 & 0 & 1 & 4 & 6 & 9 \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \\ 7 \\ 1 \end{bmatrix}$$

Observations about SIS problem

- Without constraint on $\|z\|$, it is easy to find solution via Gaussian elimination.
- If $\beta \geq q$, then $z = (q, 0, \ldots, 0) \in \mathbb{Z}^m$ is a solution.
- If z is a solution for a matrix A then z can be converted to a solution for $\left[A \mid A'\right]$ (appending z with zeros).

$$\begin{bmatrix} 1 & 4 & 5 & 9 & 3 & 0 & 2 \\ 4 & 2 & 8 & 6 & 2 & 4 & 3 \\ 7 & 5 & 5 & 4 & 7 & 8 & 0 \\ 2 & 7 & 0 & 1 & 4 & 6 & 9 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \\ 7 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix}$$

Requirements for a solution to SIS problem

The number of vectors m and the norm β must be large enough. A solution exists if

$$\beta \geq \sqrt{\lceil n \log q \rceil} \quad \text{and} \quad m \geq \lceil n \log q \rceil .$$

Proof.

w.l.o.g. assume $m = \lceil n \log q \rceil$.
Observe that

$$\left| \{x \in \{0, 1\}^m\} \right| = 2^m \geq 2^{n \log q} = q^n .$$

By the pigeonhole argument there exists $x \neq x' : Ax = Ax' \in \mathbb{Z}_q^n$.
$\Rightarrow z := x - x' \in \{0, \pm 1\}^m$ is a solution and

$$\|z\| \leq \sqrt{m} = \sqrt{\lceil n \log q \rceil} \leq \beta .$$

$\square$

Example

$q = 10, z \in \{0,1\}^m$

$$\begin{bmatrix} 1 & 4 & 5 & 9 & 3 & 0 & 2 \\ 4 & 2 & 8 & 6 & 2 & 4 & 3 \\ 7 & 5 & 5 & 4 & 7 & 8 & 0 \\ 2 & 7 & 0 & 1 & 4 & 6 & 9 \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \\ 7 \\ 1 \end{bmatrix}$$

Are the following conditions satisfied?

$$\beta \geq \sqrt{\lceil n \log q \rceil} \quad \text{and} \quad m \geq \lceil n \log q \rceil.$$

$\sqrt{7} \overset{!}{\geq} \sqrt{\lceil 4 \log 10 \rceil} = \sqrt{14}$, and $7 \overset{!}{\geq} \lceil 4 \log 10 \rceil = 14.$

Connection to Lattices

We can look at the SIS problem as a short vector problem on so-called q-ary m-dimensional lattices.

$$\mathcal{L}^{\perp}(A) := \{z \in \mathbb{Z}^m : Az = 0 \in \mathbb{Z}_q^n\} \supset q\mathbb{Z}^m.$$

Solving the SIS problems can be accomplished by finding a sufficiently short nonzero vector in $\mathcal{L}^{\perp}(A)$, where A is chosen uniformly at random.

Hardness

Theorem

For any $m = \mathrm{poly}(n)$, any $\beta > 0$, and any sufficiently large $q \geq \beta \cdot \mathrm{poly}(n)$, solving $\mathrm{SIS}_{n,q,\beta,m}$ with non-negligible probability is at least as hard as solving SIVP_γ on arbitrary n-dimensional lattices with overhelming probability, for some $\gamma = \beta \cdot \mathrm{poly}(n)$.

- Solving an arbitrary instance of a SIS problem is at least as hard as solving SIVP_γ in the worst case.
- m and q play no essential role in the hardness guarantee.
- Approximation factor γ degrades with β.

Collision Resistant Hashing

Already know that $f_A : \{0,1\}^m \to \mathbb{Z}_q^n$ is compressing provided that $m > n \log q$. The pigeonhole argument from above shows us even more. Assuming hardness of the corresponding SIS problem Ajtai's function

$$f_A : \{0,1\}^m \to \mathbb{Z}_q^n \text{ is collision resistant.}$$

Proof.

Assume to the contrary that an efficient attacker can find a collision, i.e.,

$$x \neq x' \in \{0,1\}^m : f_A(x) = f_A(x').$$

Then $z := x - x'$ is a solution for the corresponding SIS problem. $\square$

$\Rightarrow$ f_A is a collision resistant hash function.

Example: Hash-to-Point in FALCON

Input: Input string STR, modulus $q \leq 2^{16}$, degree $n \in \mathbb{N}$;
Output: polynomial $c = \sum_{i=0}^{n-1} c_i x^i \in \mathbb{Z}_q[x]$

$k \leftarrow \lfloor 2^{16}/q \rfloor$
`ctx` $\leftarrow \mathrm{SHAKE-256-Init}()$
$i \leftarrow 0$
while $i < n$ **do**
    $t \leftarrow \mathrm{SHAKE-256-Extract}(\mathrm{ctx}, 16)$
    if $t < kq$ **then**
        $c_i \leftarrow t \mod q$
        $i \leftarrow i + 1$
    end
end
return c

Commitment Scheme

Choose A_1, A_2 at random.

Commitment C to message $m \in \{0,1\}^m$:

- Choose $r \leftarrow \{0,1\}^m$
- Compute $C \leftarrow f_{[A_1,A_2]}(m,r) = A_1 m + A_2 r$

Hiding: C hides the message because $A_2 r \approx U(\mathbb{Z}_q^n)$.

Binding: Finding $(m,r) \neq (m',r')$ such that $f_{[A_1,A_2]}(m,r) = f_{[A_1,A_2]}(m',r')$ breaks the collision resistance of $f_{[A_1,A_2]}$.

Linear Homomorphism

Ajtai's function is linear homomorphic in the "message"

$$f_A(x_1 + x_2) = f_A(x_1) + f_A(x_2),$$

and the "key"

$$f_{A_1+A_2}(x) = f_{A_1}(x) + f_{A_2}(x).$$

Warning: Domain of f_A is not closed under $+$.

One-Time Signatures

f_A can be extend to matrices $X = [x_1, \ldots, x_k]$: $f_A(X) = [f_A(x_1), \ldots, f_A(x_k)] = AX(\mod q)$.

KeyGen : Let $A \in \mathbb{Z}_q^{n\times m}$ be uniformly at random. Choose $\mathsf{sk} \leftarrow (X, x) \in \{0,1\}^{k\times m} \times \{0,1\}^m$ and $\mathsf{pk} \leftarrow (Y = f_A(X), y = f_A(x))$ (image of sk under f_A).

$\mathsf{Sign}(\mathsf{sk}, m \in \{0,1\}^k)$: On input of a secret key sk and a message m, output a signature $Xm + x$.

$\mathsf{Verify}(\mathsf{pk}, m, \sigma)$: On input of a public key pk, a message m and a signature σ, return 1 if the following holds and 0 otherwise:

$$f_A(\sigma) = Ym + y.$$

Efficiency of Ajtai's function

Fix $n = 2^6$, and $q = 2^8$. How should you choose m if we aim for a efficient compression function $f_A : \{0,1\}^m \to \mathbb{Z}_q^n$? (Recall: $\beta \geq \sqrt{n \log q}$, and $m \geq n \log q$)

Key size:?

Runtime:?

Usable, but inefficient!

Summary

- SIS problem: Finding short solution in the kernel of Ajtai's function $f_A(z) := Az$.
- Solution exists if $\beta^2, m \geq n \log q$.
- SIS problem $\equiv$ SVP$_\gamma$.
- Solving average-case SIS problem is at least as hard as solving worst-case SIVP$_\gamma$.
- Ajtai's function is collision resistant.
- SIS admits minicrypt primitives (usable, but inefficient)

What you should know...

- Definition of lattices
- Computational problems: SVP_γ and SIVP_γ
- SIS problem (parameters for existence of solution, hardness, applications)