Project 1
Lattice-based Cryptography

Xiuqi Zhang Zikun Zhou Heyin Shen Anna Lee

JI SJTU

July 24, 2021

1 Introduction

2 Lattice
- Equivalent Bases
  - Column View
  - Matrix View
- Lattice meaning to space
- Successive Minima
- Gram-Schmidt Orthogonalization
- Minkowski's Theorem

3 Basic Computation Lattice Problems
- Shortest Vector Problem (SVP)
  - Hardness
  - GapSVP
- Closest vector problem (CVP)
  - Hardness

4 (Dis)Advantage of Lattice-based cryptography

5 Shortest Integer Solution Problem (SIS)
- Definition of the SIS

- One-Way & Collision-Resistant Hash Function using SIS
- Worst-case to Average-case Reduction

6 Learning With Errors Problem (LWE)

- Definition of LWE
  - Search problem
  - Decision problem
- Average Hardness

7 Ring learning with errors key exchange

8 Possible Attack for Lattice-based Cryptography

- Fault Attacks
- Effective Attacks

- A general set of cryptography that involves lattices.
- Covers encryption, signatures and hash functions.
- Post-quantum computing secure, and have proved security basing on worst-case scenario.

Introduction of Lattice

Less formally (while not indicating less accurate), lattice can be viewed as a set of points

$$L = \{a_1 v_1 + a_2 v_2 + ... + a_n v_n | a_i \in \mathbb{Z}\} \tag{1}$$

$(v_1, v_2, ..., v_n) \in \mathbb{R}^n$ and they are linear independent

Example

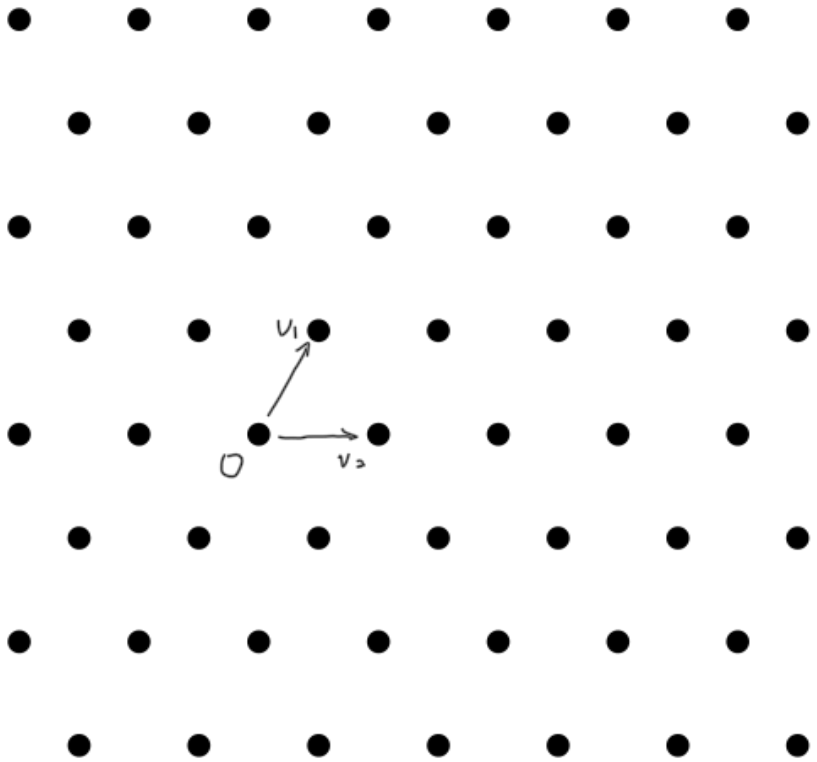

Figure: Lattice Example

Column View

- Changing order of $\forall v_i, v_j \in B$ does not chagne the lattice generated.
- $\forall v_i \in B, L(B') = L(B)$ where $B' = (B/v_i) \cup \{-v_i\}$.
- Linear Combination: for some $v_i, v_j \in B$, let $v_i = v_i + kv_j$ where $k \in \mathbb{Z}$.

Matrix view

Theorem

$$L(B_1) = L(B_2) \iff B_1 = B_2 U \tag{2}$$

where U is a unimodular U.

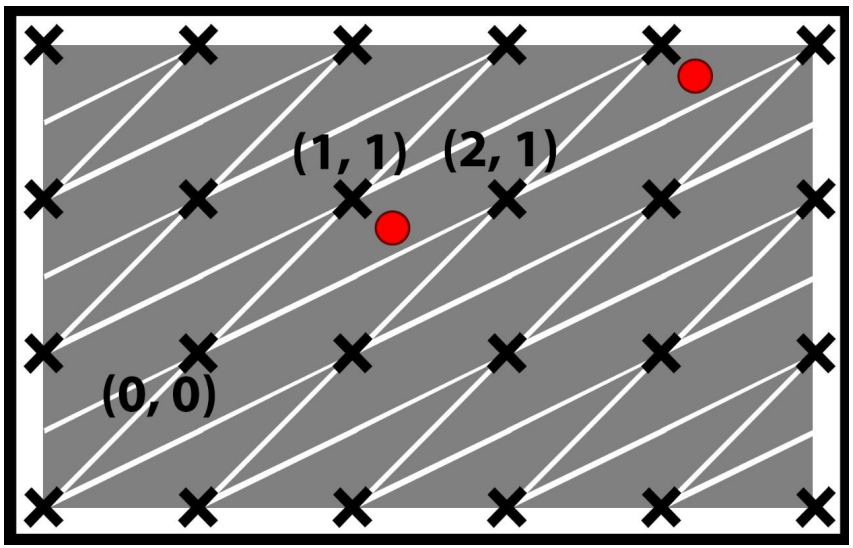

Figure: Dividing space

$L(B)$: $\det(L) = |\det(B)|$.

Successive Minima

We denote the length (Euclidean norm) of the shortest vectors in $\mathcal{L}$ as $\lambda_1(\mathcal{L})$, the second shortests as $\lambda_2(\mathcal{L})$,..., etc.

Gram-Schmidt Orthogonalization

Input: a set of linearly independent vectors
Output: a set of orthogonal vectors with same cardinality
Procedure: project each vector on the orthogonal complement of the previous vectors
Mathematical expression: for vector series $B = b_1, b_2, \ldots, b_n$, GSO vector set $\widetilde{B} = \tilde{b}_1, \tilde{b}_2, \ldots, \tilde{b}_n$ is as

$$\tilde{b}_i = b_i - \sum_{j=1}^{i-1} \mu_{i,j} \tilde{b}_j, \text{ where } \mu_{i,j} = \frac{\left\langle b_i, \tilde{b}_j \right\rangle}{\left\langle \tilde{b}_j, \tilde{b}_j \right\rangle} \tag{3}$$

Minkowski's Theorem

Theorem

Minkowski's Theorem: *For any lattice Λ and convex zero-symmetric set S, volume of which is larger than $2^n \det(\Lambda)$, there must exists some lattice point in S. (which is the upper bound of smallest lattice).*

Theorem

Inference of Minkowski's Theorem:

$$\forall \Lambda, \lambda_1(\Lambda) \leq \sqrt{n} \cdot \det(\Lambda)^{\frac{1}{n}} \tag{4}$$

From previous theorems, we know about the upper and lower bound of shortest vector, however it does not provide a way to find such vector.
This problems remain to be a hard problem, and work in the field of lattice computation problems as basic as SAT problem in NP-complete.

Hardness

In Euclidean distance, we only know that by applying randomized reductions the problem is NP-hard [2]. If considering uniform norm, the problem has already been proved to be NP-hard [1].

GapSVP

GapSVP$_\gamma$ is variant of SVP$_\gamma$, in which we try to know that whether $\lambda(\mathcal{L}(B))$ is not bigger than one, or larger than γ, where γ is some function $f(n)$, and n is the dimension of the space.
Notice that it is a promise problem, which means the input should make the result fall in one of the conditions.

Given: A basis B and a lattice L, and some vector $v \in \vec{(}B)$.
Try to find: A vector $v' \in L$, which is closest to v.

Hardness

Conclusion: We can solve SVP efficiently if we can solve CVP.
Further thought: Goldreich et al. proved that CVP is at least harder than SVP at any aspect [3], and Dinur et al. proved that, with factor $n^{c/\log\log n}$ for some constant $c > 0$, CVP is NP-hard to approximate [5].

Advantages

1. Anti-quantum attack
   Traditional public-key cryptographies are solvable in the context of the modern quantum algorithm, while lattice-based cryptographies are not.
2. Efficient algorithm and high concurrency
   Calculations in cryptosystems are based on the manipulation of vectors without the engagement of large prime integers.
3. Worst case to average case reduction
   The lattice-based cryptography is built based on the "worst case to average case reduction". In contrast, cryptographies that are based on factoring, though hard in the worst case, can still be decrypted easily if it is easy to solve on average input.

Disadvantages

1. Large length of the private key
   The existing lattice-based cryptosystem suffers from an unsatisfactorily large length of the private key.
2. Further improvement
   Though this situation has progressed, there still remains room for further improvement.

Definition

Given m random vectors $a_1, a_2, ..., a_m$ in Z_q^n (e.g., $q \approx n^3$), find a non-trivial solution $z_1, z_2, ..., z_m$ in $\{-1, 0, 1\}$ such that:

$$z_1 \cdot \begin{pmatrix} | \\ a_1 \\ | \end{pmatrix} + z_2 \cdot \begin{pmatrix} | \\ a_2 \\ | \end{pmatrix} + \cdots + z_m \cdot \begin{pmatrix} | \\ a_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ 0 \\ | \end{pmatrix} \in Z_q^n \quad (5)$$

Denote $\mathrm{A} = (a_1, a_2, ..., a_m)$ and $\mathrm{Z} = z_1, z_2, ..., z_m$:

$$\begin{pmatrix} \cdots & \mathrm{A} & \cdots \end{pmatrix} \begin{pmatrix} \\ \mathrm{z} \\ \end{pmatrix} = 0 \in Z_q^n \quad (6)$$

Hash Function

An one-way & collision-resistant hash function can be easily implied from the SIS:
Set $m > n \lg q$. Given random A in $\mathbb{Z}_q^{n \times m}$, define the hash function $f_A : \{0,1\}^m \to \mathbb{Z}_q^n$ as:

$$f_A(z) = Az \tag{7}$$

A collision $f_A(z) = f_A(z')$ yields a solution $z - z'$ of the SIS for A, as $z - z'$ is in $\{0,1\}^m$ and satisfy $A(z - z') = 0$

Uniform Distribution Over Lattices

Theorem

Consider a Gaussian distribution:

$$\rho_s(x) = (1/s)e^{-\pi x^2/s^2} \tag{8}$$

and s=5M, for some positive M, if $X \sim \rho_s$*, then for all* $m < M$*:*

$$\Delta(X \mod m, \mathrm{Uniform}[0, m)) < 2^{-110} \tag{9}$$

Lemma

If $s > 5\lambda_n(\mathrm{B})$*, and* $\mathrm{X} \sim \rho_s(\mathrm{x}) = (1/s)^n e^{-\pi||\mathrm{x}||^2/s^2}$*, then*

$$\Delta(\mathrm{X} \mod \mathrm{B}, \mathrm{Uniform}(\mathrm{B})) < n2^{-110} \tag{10}$$

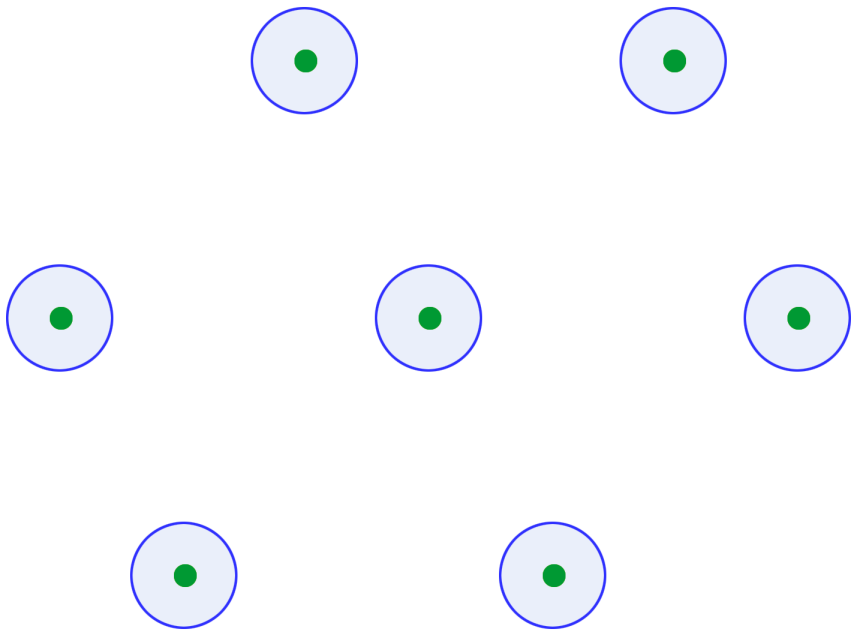

Figure: The distribution when s is small

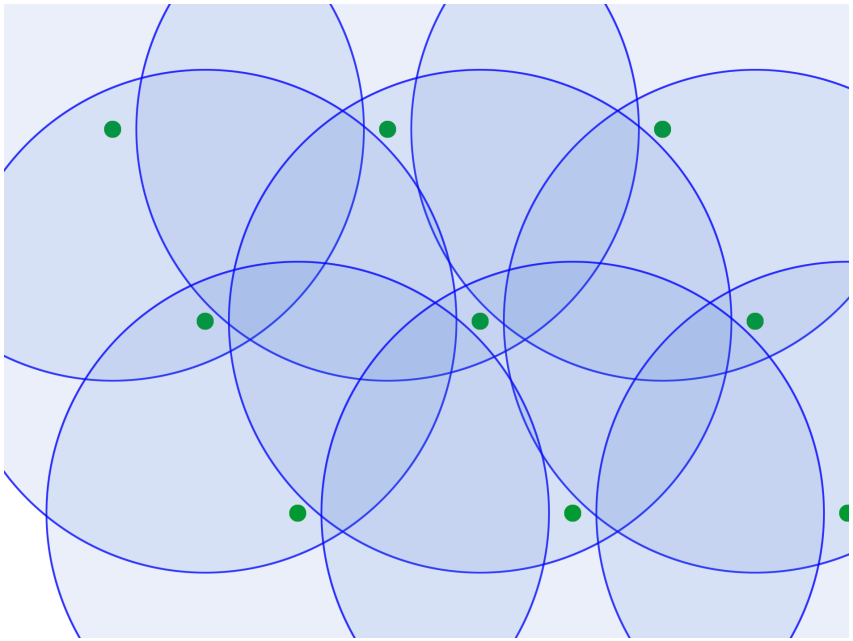

Figure: The distribution when s increases

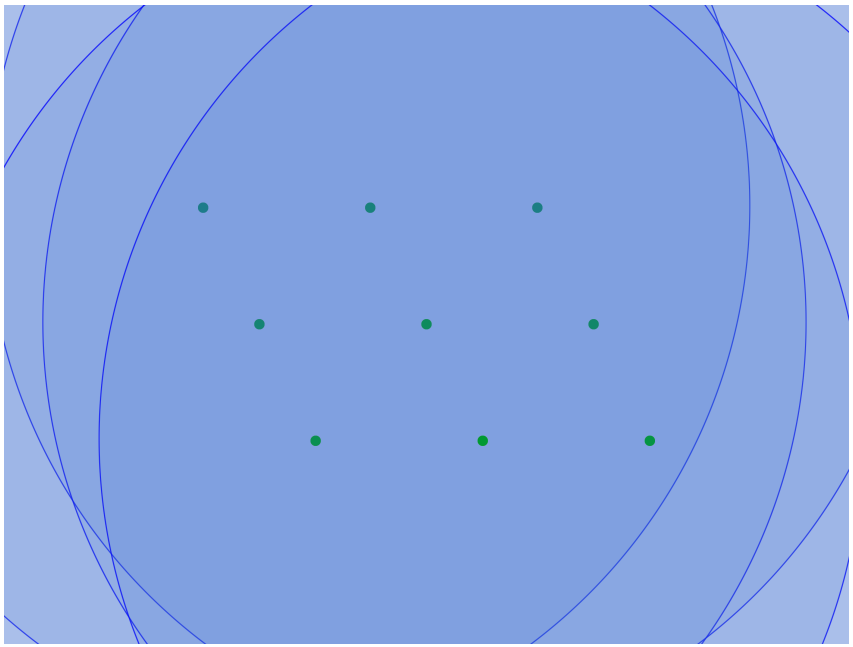

Figure: The distribution when s is large enough

Reduction

Algorithm 1 Solving SVP using SIS oracle

for m times **do**
  Pick a random lattice point v_i
  Gaussian sample a point $a_i = v_i + r_i$ round to $\mathbb{Z}_q^n$ around v_i
end for
A $= (a_1, a_2, ..., a_m) \rightarrow$ SIS oracle
SIS oracle $\rightarrow$ z
Output the short lattice vector: Rz

1. $A = (a_1, a_2, ..., a_m)$ is uniformly random in Z_q^n, Therefore, we can give A to the SIS oracle.
2. The SIS oracle will output the solution of $Az = 0$. Let $V = v_1, ..., v_m$ and $R = r_1, ..., r_m$, $Az = 0$ is a zero vector which is a lattice vector in $L(B)$ and Vz is a lattice vector. Therefore, Rz is also a lattice vector.
3. As $z \in \{-1, 0, 1\}^m$ and r_i is short, Rz is a short lattice vector which is the solution of the SVP.

Consider an additive group $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ which is constructed modulo one. For error, produce a fixed probability distribution over $\mathbb{T}$ denoted as φ.
We than define a distribution over $\mathbb{Z}_q^n \times \mathbb{T}$ as

1. Randomly get a vector $a \in \mathbb{Z}_q^n$ following uniform distribution.
2. Randomly get a number $\epsilon \in \mathbb{T}$ following distribution φ.
3. Compute addition and division under $\mathbb{T}$, inner product in $\mathbb{Z}_q^n$ calculate $t =< a, s > /q + e$.
4. Pair (a, t) is a sample.

Denote the entire sample set as $A_{s,\varphi}$.

With above definition, we define the LWE search problem as trying to find s, given polynomial amout of samples from $A_{s,\varphi}$. Most times we studied a special case of LWE, where φ is the nomal distrubtion as origin point with variance of $\frac{\alpha^2}{2\pi}$, i.e. $e^{-\pi(|x|/\alpha)^2}/\alpha$.

On the other hand, LWE decision problem is to tell the difference between a LWE distributed input and a uniformly random input.

Peikert proved that the worst case of LWE can be reduced to GapSVP in polynomial time, considering a approximate output [8].

Ring learning with errors key exchange

The ring learning with errors key exchange is a typical example of the lattice-based cryptosystem, which has the speciality to be reduced to known hard problem.

Algorithm

Algorithm 2 Initiation

s_l, $e_l \leftarrow$ *polynomials with coefficients from* χ_α *distribution*
$p_l \leftarrow as_l + 2e_l$
return p_l

Algorithm 3 Response

$E \leftarrow \left\{-\left\lfloor \frac{q}{4} \right\rfloor, \ldots, \left\lfloor \frac{q}{4} \right\rfloor\right\} ofZq = \left\{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\right\}$

$s_R, e_R \leftarrow$ *polynomials with coefficients from* χ_α *distribution*

$p_R \leftarrow as_R + 2e_R$

$e'_R \leftarrow samplefrom\chi_\alpha$ *distribution*

$k_R \leftarrow p_I s_R + 2e'_R$

for each coefficient k_{R_i} of k_R **do**

  if $k_{R_i} \in E$ **then**

    $w_i \leftarrow 0$

  else

    $w_i \leftarrow 1$

  end if

end for

$sk_R = \left(k_R + w \cdot \frac{q-1}{2}\right) \bmod q \bmod 2$

return p_R, w

Fault Attacks

1. Loop-Abort Faults on Lattice-based Signature [4]
   Fiat-Shamir family By inputing a fault in the loop, they could get the commitment value, which is a random polynomial.
   GPV-based hash-and-sign signature When it is applied into the early loop abort, the original ciphertext will become a linear combination of the parts of the secret lattice.
2. "Fiat-Shamir with Aborts" Framework
   By using a "skipaddition" attack, the attacker could retrieve the primary secret. Then the attack could make a forgery attack on the Dilithium signature scheme.

Effective Attacks

1. Physical attack
   There are little research results on the physical security of lattice-based cryptography. And, physical attack is easier comparing to other attack. [4]
2. Cryptanalysis of GGH [6]
   Use the specific modular operations: they could reduce the effect of noise of GGH.
   Use the hardness of exact-3-call problem: they can break WE(witness encryption).
3. Attack against Cai-Cusick
   Cai-Cusick is a lattice-based public-key cryptosystem. Has little data expansion. Yanbin Pan and Yingpu Deng proposed a way of ciphertext-only attack towards the Cai-Cusick crypto system. [7]

Algorithm

Algorithm $\mathcal{A}$. The Ciphertext-Only Attack

Input: The public key $v_{\sigma(0)}, v_{\sigma(1)}, \ldots, v_{\sigma(m)}, b$ and any ciphertext C.

Output: The corresponding message $M = (a_0, a_1, \ldots, a_m)$ or "Failure."

1: Compute the Gram-Schmidt orthogonalization vectors $v^*_{\sigma(0)}, v^*_{\sigma(1)}, \ldots, v^*_{\sigma(m)}$.
2: If $\min_{0 \le i \le m} \|v^*_{\sigma(i)}\| \le b$, output "Failure" and halt, else do $3 - 8$.
3: $i := m$.
4: **Repeat**
5: Compute $a_i := \lceil \frac{\langle v^*_{\sigma(i)}, C \rangle}{\|v^*_{\sigma(i)}\|^2} \rfloor$.
6: $C := C - a_i v_{\sigma(i)}$, $i := i - 1$.
7: **Until** $i < 0$.
8: **Return** $(a_0, a_1, \ldots, a_m)$.

[1] M. Ajtai.
Generating hard instances of lattice problems (extended abstract).
In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 99–108, New York, NY, USA, 1996. Association for Computing Machinery.

[2] Miklós Ajtai.
The shortest vector problem in l2 is np-hard for randomized reductions (extended abstract).
In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, page 10–19, New York, NY, USA, 1998. Association for Computing Machinery.

[3] I. Dinur, G. Kindler, R. Raz, and S. Safra.
Approximating cvp to withinalmost-polynomial factors is np-hard.
Combinatorica, 23(2):205–243, 2003.

[4] Thomas Espitau, Pierre-Alain Fouque, Benoit Gerard, and Mehdi Tibouchi.
Loop-abort faults on lattice-based signature schemes and key exchange protocols.
IEEE Transactions on Computers, 67(11):1535–1549, 2018.

[5] Oded Goldreich, Daniele Micciancio, Shmuel Safra, and Jean-Pierre Seifert.
Approximating shortest lattice vectors is not harder than approximating closest lattice vectors.
Information Processing Letters, 71(2):55–61, 1999.

[6] Yupu Hu and Huiwen Jia.
Cryptanalysis of ggh map.
IEEE Transactions on Computers, 67(11):1535–1549, 2018.

[7] Yanbin Pan and Yingpu Deng.
A ciphertext-only attack against the cai-cusick lattice-based public-key cryptosystem.
IEEE TRANSACTIONS ON INFORMATION THEORY, 57(3):1780–1785, 2011.

[8] Chris Peikert.
Public-key cryptosystems from the worst-case shortest vector problem: Extended abstract.
In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, page 333–342, New York, NY, USA, 2009. Association for Computing Machinery.