1 Introduction

Definition 1.1 A lattice $L \subseteq \mathbb{R}^n$ is a set of points defined as:

$$L = \{ \sum_{i=1}^{m} \alpha_i u_i \mid \alpha_i \in \mathbb{Z} \text{ and } u_i \in \mathbb{R}^n \}$$

We will assume that $m = n$ and $u_i$'s are linearly independent. The problem of computing a shortest vector in a given lattice is $\text{NP}$-hard. We define the volume of a lattice $L$ as:

$$\text{Vol}(L) = |\text{det}[u_1 \ u_2 \ \ldots \ u_n]|$$

If the $u_i$'s are linearly dependent then $\text{Vol}(L) = 0$. The vectors $u_1, u_2, \ldots, u_n$ are called a basis for $L$.

Lemma 1.1 $\text{Vol}(L)$ is independent of the choice of the basis.

Proof. Let $v_1, v_2, \ldots, v_n$ be another basis for $L$. We have, $v_j = \sum_{i=1}^{n} \beta_{ij} u_i$, where $\beta_{ij} \in \mathbb{Z}$.

$$[v_1 \ v_2 \ \ldots \ v_n] = [u_1 \ u_2 \ \ldots \ u_n] \cdot [\beta_{ij}]$$
$$\Rightarrow |\text{det}[v_1 \ v_2 \ \ldots \ v_n]| = |\text{det}[u_1 \ u_2 \ \ldots \ u_n]| \cdot |\text{det}[\beta_{ij}]|$$
$$\Rightarrow |\text{det}[u_1 \ u_2 \ \ldots \ u_n]| \mid \text{divides} \ |\text{det}[v_1 \ v_2 \ \ldots \ v_n]|$$

Similarly, $|\text{det}[v_1 \ v_2 \ \ldots \ v_n]| \mid \text{divides} \ |\text{det}[u_1 \ u_2 \ \ldots \ u_n]|$.

Therefore, $|\text{det}[v_1 \ v_2 \ \ldots \ v_n]| \mid \text{divides} \ |\text{det}[u_1 \ u_2 \ \ldots \ u_n]|$.

2 Application of finding Short Vector in a Lattice

Consider the scenario where the RSA cryptosystem is used. Let $p$ and $q$ be two large primes and $n = pq$. Let $(n, 3)$ be the public key. Suppose we encrypt message $m$ such that the initial part of $m$ is a fixed header $h$ that is known, whereas the unknown content of the message be $x$ that is $l$ bits long. Without loss in generality assume that $0 \leq m < n$. 


Let $m = h \cdot 2^l + x$ and $c = m^3 (mod n)$. Assume that the adversary knows $c$, $h$, $l$ and $(n, 3)$. Since,

\[ c = (h \cdot 2^l + x)^3 (mod n) \]

\[ \Rightarrow p(x) = x^3 + a_2 x^2 + a_1 x + (a_0 - c) = 0 (mod n) \]

The adversary computes $p(x)$ and tries to solve for $x$. Let a lattice $L \in \mathbb{R}^6$ be defined by the following basis vectors:

\[
\begin{pmatrix}
  a_0 - c \\
  a_1 \\
  a_2 \\
  1 \\
  0 \\
  0
\end{pmatrix},
\begin{pmatrix}
  0 \\
  a_0 - c \\
  a_1 \\
  a_2 \\
  1 \\
  0
\end{pmatrix},
\begin{pmatrix}
  0 \\
  0 \\
  a_0 - c \\
  a_1 \\
  a_2 \\
  1
\end{pmatrix},
\begin{pmatrix}
  n \\
  0 \\
  0 \\
  0 \\
  0 \\
  0
\end{pmatrix},
\begin{pmatrix}
  0 \\
  n \\
  0 \\
  0 \\
  0 \\
  0
\end{pmatrix},
\begin{pmatrix}
  0 \\
  0 \\
  0 \\
  0 \\
  n \\
  nx^2
\end{pmatrix}
\]

Therefore, $Vol(L) = n^3$.

**Theorem 2.1 (Minkowski)** Let $L \in \mathbb{R}^d$ be a lattice. Then, the length of the shortest vector in $L \leq d^{\frac{1}{2}} \cdot Vol(L)^{\frac{1}{2}}$.

From the above theorem we conclude that the shortest vector in our lattice $L$ has length $\leq \sqrt{6n^2}$.

Let $v = (v_0, v_1, \ldots, v_5)$ be the shortest vector in $L$. Let the polynomial

\[ v(x) = \sum_{i=0}^{5} v_i x^i \]

\[ = \gamma_1 p(x) + \gamma_2 x p(x) + \gamma_3 x^2 p(x) + \gamma_4 n + \gamma_5 nx + \gamma_6 nx^2 \]

\[ = (\gamma_1 + \gamma_2 x + \gamma_3 x^2) p(x) (mod n) \]

Suppose $x = m_0$ be the unknown message. Then

\[ p(m_0) = 0 (mod n) \]

\[ \Rightarrow v(m_0) = 0 (mod n) \]

\[ \Rightarrow m_0 \text{ is a root of } v(x) \text{ modulo } n \]

\[ | v(m_0) | = \left| \sum_{i=0}^{5} v_i m_0^i \right| \]
\[ \leq 6 \max \{ |v_i| \} m_0^5 \]
\[ \leq 6 \max \{ |v_i| \} 2^{5l} \]
\[ \leq 6 \sqrt{6} \cdot \sqrt{n} \cdot 2^{5l} \]
\[ < n \text{ if } l < \frac{1}{10} \log \frac{n}{216} \]
Therefore, $v(m_0) = 0$ over $\mathbb{Z}$. Thus if the actual message $x$ is only about $\frac{1}{10}$th of the total message then the adversary can solve for $x$ by computing a shortest vector $v$ in $L$ and then solving for $v(x) = 0$ over $\mathbb{Z}$. 