Learning with error was proposed by O. Regev in 2005 (see Regev, 2009), which can be regarded as a dual form of SIS problem. LWE has very important applications in modern cryptography, such as LWE-based fully homomorphic encryption. The main purpose of this chapter is to explain the mathematical principles of the LWE problem in detail, especially the polynomial equivalence between the average LWE problem and the hard problems on lattice, which is one generalization of the Ajtai reduction principle and solves the computational complexity of the LWE problem effectively.

3.1 Circulant Matrix

Circulant matrix is a kind of simple and beautiful special matrix in mathematics, which has important applications in many fields of engineering technology. In Sect. 7.7 of ‘Modern Cryptography’, we explain and demonstrate the basic properties of circulant matrix in detail. See the monograph Zheng (2022) on circulant matrices for more details.

Let $T$ be a square matrix of order $n$,

$$T = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 \\ I_{n-1} & \cdots & 0 \\ 0 & \cdots & I_{n-1} \\ \end{pmatrix}_{n \times n},$$

(3.1.1)

where $I_{n-1}$ is the $n - 1$ dimensional unit matrix. Obviously, we can define a linear transformation $x \to Tx$, $x \in \mathbb{R}^n$ of $\mathbb{R}^n \to \mathbb{R}^n$ by $T$. The characteristic polynomial of $T$ is $f(x) = x^n - 1$, so $T^n = I_n$. We use column notation for vectors in $\mathbb{R}^n$, and $\{e_0, e_1, \ldots, e_{n-1}\}$ is the standard basis of $\mathbb{R}^n$, i.e.
\[
e_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad e_{n-1} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.
\]

(3.1.2)

Denote \( e_m \) as \( e_k \) if \( m \equiv k \pmod{n} \), and \( 0 \leq k \leq n-1 \), it is easy to see
\[
Te_k = e_{k+1}, \quad \text{and} \quad T^k(e_0) = e_k, \quad 0 \leq k \leq n-1.
\]

(3.1.3)

**Definition 3.1.1** Let \( \alpha = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} \in \mathbb{R}^n \), the circulant matrix \( T^*(\alpha) \) generated by \( \alpha \) is defined by
\[
T^*(\alpha) = [\alpha, T\alpha, \ldots, T^{n-1}\alpha]_{n\times n} \in \mathbb{R}^{n\times n}.
\]

(3.1.4)

It is easy to verify that the circulant matrix \( B \) generated by the linear combination \( \alpha \) is the linear combination of the corresponding circulant matrices, i.e.
\[
T^*(a\alpha + b\beta) = aT^*(\alpha) + bT^*(\beta).
\]

(3.1.5)

Specially, for any \( \alpha = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} \in \mathbb{R}^n \), the circulant matrix \( T^*(\alpha) \) generated by \( \alpha \) could be written as
\[
T^*(\alpha) = T^* \left( \sum_{i=0}^{n-1} \alpha_i e_i \right) = \sum_{i=0}^{n-1} \alpha_i T^*(e_i),
\]

(3.1.6)

therefore, any circulant matrix is the linear combination of circulant matrices generated by the standard basis vectors \( e_i \). It is easy to verify that
\[
T^*(e_k) = T^k, \quad 0 \leq k \leq n-1.
\]

(3.1.7)

In particular, the unit matrix \( I_n \) is a circulant matrix generated by the vector \( e_0 \). The basis properties about the circulant matrix are summarized in the following lemma, and the corresponding proofs could be found in Sect. 7.7 in Zheng (2022).

**Lemma 3.1.1** Let \( \alpha = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix}, \quad \beta = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{n-1} \end{pmatrix} \) be two vectors in \( \mathbb{R}^n \), then we have
(i) \( T^*(\alpha) = \alpha_0 I_n + \alpha_1 T + \cdots + \alpha_{n-1} T^{n-1}. \)

(ii) \( T^*(\alpha) \cdot T^*(\beta) = T^*(\beta) \cdot T^*(\alpha). \)

(iii) \( T^*(\alpha) \cdot T^*(\beta) = T^*(T^*(\alpha) \beta). \)

(iv) \( \det(T^*(\alpha)) = \prod_{i=0}^{n-1} \alpha(w_i), \) where \( w_i \) is the \( n \)-th unit root.

(v) \( T^*(\alpha) \) is an invertible matrix if and only if the characteristic polynomial \( \alpha(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1} \) corresponding to \( \alpha \) and \( x^n - 1 \) are coprime, i.e. \( (\alpha(x), x^n - 1) = 1. \)

We take the characteristic polynomial \( x^n - 1 \) as modulo and construct the one-to-one correspondence between polynomial quotient rings and \( n \) dimensional vectors, which is called the geometric theory of polynomial rings. We consider the following three polynomial quotient rings. Let \( \mathbb{R}[x], \mathbb{Z}[x] \) and \( \mathbb{Z}_q[x] \) be the polynomial rings of one variable on \( \mathbb{R}, \mathbb{Z} \) and \( \mathbb{Z}_q \) respectively, defined by

\[
\overline{R} = \mathbb{R}[x]/<x^n - 1> = \left\{ \sum_{i=0}^{n-1} a_i x^i \mid a_i \in \mathbb{R} \right\}, \quad (3.1.8)
\]

\[
R = \mathbb{Z}[x]/<x^n - 1> = \left\{ \sum_{i=0}^{n-1} a_i x^i \mid a_i \in \mathbb{Z} \right\}, \quad (3.1.9)
\]

and

\[
R_q = \mathbb{Z}_q[x]/<x^n - 1> = \left\{ \sum_{i=0}^{n-1} a_i x^i \mid a_i \in \mathbb{Z}_q \right\}. \quad (3.1.10)
\]

In fact, the right hand side of the above formula is a set of representative elements of the polynomial quotient ring.

For any \( \alpha(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1} \in \overline{R} \), we construct the following correspondence

\[
\alpha(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1} \in \overline{R} \leftrightarrow \alpha = \begin{pmatrix} 
\alpha_0 \\
\alpha_1 \\
\vdots \\
\alpha_{n-1} 
\end{pmatrix} \in \mathbb{R}^n, \quad (3.1.11)
\]

written as \( \alpha(x) \leftrightarrow \alpha \) or \( \alpha \leftrightarrow \alpha(x) \). Then (3.1.11) gives a one-to-one correspondence between \( \overline{R} \) and \( \mathbb{R}^n \). In the same way, \( \alpha(x) \leftrightarrow \alpha \) also gives the one-to-one correspondences of \( R \to \mathbb{Z}^n \) and \( R_q \to \mathbb{Z}_q^n \). It is not hard to see that the above correspondence is an Abel group isomorphism. To establish ring isomorphism, we introduce the concept of convolution multiplication of vectors.

**Definition 3.1.2** For any two vectors \( \alpha, \beta \) in \( \mathbb{R}^n, \mathbb{Z}^n \) or \( \mathbb{Z}_q^n \), we define the convolution \( \alpha \otimes \beta \) by

\[
\alpha \otimes \beta = T^*(\alpha) \cdot \beta. \quad (3.1.12)
\]
Under the above definition, $\mathbb{R}^n$, $\mathbb{Z}^n$ and $\mathbb{Z}^n_q$ become a commutative ring with unit element, respectively. Obviously, the convolution defined by (3.1.12) is closed on $\mathbb{Z}^n$ or $\mathbb{Z}^n_q$. If $\alpha \in \mathbb{Z}^n$, then $T^*(\alpha) \in \mathbb{Z}^{n\times n}$, thus, $\alpha \otimes \beta = T^*(\alpha)\beta \in \mathbb{Z}^n$, so is $\mathbb{Z}^n_q$. Based on the property (iii) of lemma 3.1.1,

$$T^*(\alpha \otimes \beta) = T^*(T^*(\alpha)\beta) = T^*(\alpha)T^*(\beta) = T^*(\beta)T^*(\alpha) = T^*(\beta \otimes \alpha),$$

so we have $\alpha \otimes \beta = \beta \otimes \alpha$. On the other hand,

$$((\alpha + \alpha') \otimes \beta) = T^*(\alpha + \alpha')\beta = T^*(\alpha)\beta + T^*(\alpha')\beta = \alpha \otimes \beta + \alpha' \otimes \beta,$$

hence, $\mathbb{R}^n$, $\mathbb{Z}^n$ and $\mathbb{Z}^n_q$ are commutative rings with the same unit element $e_0$. Since $T^*(e_0) = I_n$, then

$$e_0 \otimes \beta = T^*(e_0)\beta = I_n\beta = \beta.$$

**Lemma 3.1.2** Suppose $\mathcal{R}$, $R$ and $R_q$ are defined by (3.1.8), (3.1.9) and (3.1.10), then we have the following three ring isomorphisms:

$$\mathcal{R} \cong \mathbb{R}^n, \ R \cong \mathbb{Z}^n \text{ and } R_q \cong \mathbb{Z}^n_q.$$ 

**Proof** We only prove $\mathcal{R} \cong \mathbb{R}^n$, the other two conclusions could be proved in the same way. $\forall \alpha(x) \in \mathcal{R}$, $\alpha(x) \longleftrightarrow \alpha \in \mathbb{R}^n$ is a one-to-one correspondence and an Abel group isomorphism. We are to prove

$$\alpha(x)\beta(x) \longleftrightarrow \alpha \otimes \beta, \ \forall \alpha(x), \beta(x) \in \mathcal{R}. \quad (3.1.13)$$

Let $\beta(x) = \beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1}$, then

$$x\beta(x) = \beta_0 x + \beta_1 x^2 + \cdots + \beta_{n-2} x^{n-1} + \beta_{n-1} x^n$$

$$= \beta_{n-1} + \beta_0 x + \cdots + \beta_{n-2} x^{n-1},$$

so $x\beta(x) \longleftrightarrow T\beta$. For all $k$, $0 \leq k \leq n - 1$, we know

$$x^k \beta(x) \longleftrightarrow T^k \beta.$$ 

Let $\alpha(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1}$, it follows that

$$\alpha(x)\beta(x) = \sum_{k=0}^{n-1} \alpha_k x^k \beta(x) \longleftrightarrow \sum_{k=0}^{n-1} \alpha_k T^k \beta = T^*(\alpha)\beta = \alpha \otimes \beta.$$

Therefore, we prove that $\mathcal{R} \cong \mathbb{R}^n$. Similarly, we have $R \cong \mathbb{Z}^n$ and $R_q \cong \mathbb{Z}^n_q$. $\square$

Since $\mathbb{R}^n$ is Euclidean space, the Euclidean distances in $\mathbb{Z}^n$ and $\mathbb{Z}^n_q$ could also be defined as the Euclidean distance in $\mathbb{R}^n$, which is called the embedding of Euclidean
distance in $\mathbb{Z}^n$ and $\mathbb{Z}_q^n$. By Lemma 3.1.2, we treat $\mathbb{R}$, $R_q$ and $\mathbb{R}^n$, $\mathbb{Z}^n$, $\mathbb{Z}_q^n$ as the same and write $\mathbb{R} = \mathbb{R}^n$, $R = \mathbb{Z}^n$, $R_q = \mathbb{Z}_q^n$. Therefore, the polynomial rings $\mathbb{R}$, $R$ and $R_q$ also have Euclidean distance, which constructs the geometry of the polynomial ring. For any polynomial $\alpha(x) \in \mathbb{R}$, we define

$$|\alpha(x)| = |\alpha|, \text{ if } \alpha(x) \longleftrightarrow \alpha.$$  \hspace{1cm} (3.1.14)

**Lemma 3.1.3**  For any $\alpha(x), \beta(x) \in \mathbb{R}$ (or $R, R_q$), we have

$$|\alpha(x)\beta(x)| \leq \sqrt{n}|\alpha(x)| \cdot |\beta(x)|.$$  

**Proof**  To prove this lemma, we only prove that for any $\alpha, \beta \in \mathbb{R}^n$ (the same as $\mathbb{Z}^n$ or $\mathbb{Z}_q^n$), we have

$$|\alpha \otimes \beta| \leq \sqrt{n}|\alpha| \cdot |\beta|.$$  \hspace{1cm} (3.1.15)

By Definition 3.1.2,

$$\alpha \otimes \beta = T^*(\alpha)\beta = [\alpha, T\alpha, \ldots, T^{n-1}\alpha] \beta = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{R}^n.$$

Let $\overline{\alpha}$ be the conjugation vector of $\alpha$, i.e.

$$\alpha = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} \Rightarrow \overline{\alpha} = \begin{pmatrix} \alpha_{n-1} \\ \alpha_{n-2} \\ \vdots \\ \alpha_0 \end{pmatrix},$$

then, the circulant matrix $T^*(\alpha)$ generated by $\alpha$ can be divided into rows

$$T^*(\alpha) = \begin{pmatrix} \overline{\alpha}^T T \\ \overline{\alpha}^T (T^T)^2 \\ \vdots \\ \overline{\alpha}^T (T^T)^n \end{pmatrix}.$$  

where $T^T$ is the transposed matrix of $T$. So $b_i = \overline{\alpha}^T (T^T)^i \beta$ ($1 \leq i \leq n$) and we get

$$|b_i| \leq |\alpha| \cdot |\beta|, \ 1 \leq i \leq n.$$
It follows that
\[ |\alpha \otimes \beta| = \left( \sum_{i=1}^{n} b_i^2 \right)^{\frac{1}{2}} \leq \sqrt{n} |\alpha| \cdot |\beta|. \]

We complete the proof. \( \square \)

Finally we discuss the relation between circulant matrix and lattice. Let \( B \in \mathbb{R}^{n \times n} \) be a square matrix of order \( n \), the lattice \( L(B) \subset \mathbb{R}^n \) generated by \( B \) is defined by
\[ L(B) = \{ Bx \mid x \in \mathbb{Z}^n \}. \]

If \( B \) is an invertible matrix, then \( L(B) \) is called an \( n \) dimensional full rank lattice.

**Definition 3.1.3** Let \( L(B) \subset \mathbb{R}^n \) be a lattice, we call \( L(B) \) a cyclic lattice, if \( L(B) \) is closed under the linear transformation \( T \), i.e. for any \( \alpha \in L(B) \) we have \( T\alpha \in L(B) \).

If \( L(B) \subset \mathbb{Z}^n \) is a cyclic lattice, then \( L(B) \) is called a cyclic integer lattice.

**Lemma 3.1.4** Let \( \alpha \in \mathbb{R}^n \), then the lattice \( L(T^*(\alpha)) \) generated by the circulant matrix \( T^*(\alpha) \) is a cyclic lattice, which is the smallest cyclic lattice containing \( \alpha \).

**Proof** Based on the definition \( T^*(\alpha) = [\alpha, T\alpha, \ldots, T^{n-1}\alpha] \), we get
\[ L(T^*(\alpha)) = \left\{ \sum_{i=0}^{n-1} a_i T^i \alpha \mid a_i \in \mathbb{Z} \right\}. \]

For any \( \beta \in L(T^*(\alpha)) \),
\[ \beta = \sum_{i=0}^{n-1} b_i T^i \alpha \Rightarrow T\beta \in L(T^*(\alpha)), b_i \in \mathbb{Z}, \]

so \( L(T^*(\alpha)) \) is a cyclic lattice. Assume \( L \) is a cyclic lattice containing \( \alpha \), since \( \alpha \in L \), \( T\alpha \in L \), \( T^2\alpha \in L \), ..., \( T^{n-1}\alpha \in L \), then any linear combination of integer coefficients
\[ \sum_{i=0}^{n-1} a_i T^i \alpha \in L \Rightarrow L(T^*(\alpha)) \subset L. \]

This means that \( L(T^*(\alpha)) \) is the smallest cyclic lattice containing \( \alpha \). \( \square \)

**Lemma 3.1.5** Let \( L(B) \subset \mathbb{R}^n \) be a cyclic lattice, \( \alpha \in L(B) \) be a lattice vector, then there is an integer matrix \( D \in \mathbb{Z}^{n \times n} \) such that
\[ T^*(\alpha) = BD. \quad (3.1.16) \]

**Proof** Since \( \alpha \in L(B) \), \( L(B) \) is a cyclic lattice, then \( T\alpha \in L(B), T^2\alpha \in L(B), \ldots, T^{n-1}\alpha \in L(B) \). Let \( (0 \leq k \leq n - 1) \)
the circulant matrix $T_k(\alpha)$ generated by $\alpha$ could be written as

$$T_k(\alpha) = [\alpha, T\alpha, \ldots, T^{n-1}\alpha] = Bd_0, Bd_1, \ldots, Bd_{n-1} = BD.$$
(1) Rounding off (see Theorem 7 of Chap. 7 in Zheng (2022))

∀ \( x \in \mathbb{R}^n \), let 
\[ x = \sum_{i=1}^n x_i \beta_i^* \]
where \( x_i \in \mathbb{R} \). Define \( \delta_i \in \mathbb{Z} \) is the nearest integer of \( x_i \), and
\[ [x]_B = \sum_{i=1}^n \delta_i \beta_i^* \quad \{x\}_B = \sum_{i=1}^n a_i \beta_i^* , \quad -\frac{1}{2} < a_i \leq \frac{1}{2} , \quad 1 \leq i \leq n. \]

It is easy to see \( x = [x]_B + \{x\}_B \), where \([x]_B \in L\) is a lattice vector.

(2) Nearest plane

Let \( U = L(\beta_1, \beta_2, \ldots, \beta_{n-1}) \subset \mathbb{R}^n \) be an \( n-1 \) dimensional subspace, 
\[ L' = \sum_{i=1}^{n-1} \mathbb{Z}\beta_i \subset L \text{ is a sublattice of } L. \]

After \( x \in \mathbb{R}^n \) is given, let \( v \in L \), such that \( U + v \) is the nearest plane of \( x \). Let \( x' \) be the orthographic projection of \( x \) in \( U + v \), \( y \in L' \) be the nearest lattice vector of \( x - v \), \( w = y + v \) be an approximation of the nearest lattice vector of \( x \) in \( L \). Based on the above definitions, we can prove that (see (7.82) of Chap. 7 in Zheng (2022))

\[
\begin{align*}
U &= L(\beta_1, \beta_2, \ldots, \beta_{n-1}) = L(\beta_1^*, \beta_2^*, \ldots, \beta_{n-1}^*) \\
v &= \delta_n \beta_n \in L \\
x' &= \sum_{i=1}^{n-1} x_i \beta_i^* + \delta_n \beta_n^* \\
y &= \text{the nearest lattice vector of } x - v \text{ in } L' \\
w &= y + v \in L \\
\end{align*}
\]

(3.1.22)

Since \( v = \delta_n \beta_n, x' = \sum_{i=1}^{n-1} x_i \beta_i^* + \delta_n \beta_n^* \), 
\[ |x - x'| = |x_n - \delta_n| |\beta_n^*| \leq \frac{1}{2} |\beta_n^*|. \]

The distance between any two planes in \( \{ U + z \mid z \in L \} \) is at least \( |\beta_n^*| \), and \( |x - x'| \) is the distance of \( x \) from the nearest plane, so we have 
\[ |x - x'| \leq |x - u_x|. \]

Let \( w = y + v = y + \delta_n \beta_n \in L \), we are to prove 
\[ |x - w|^2 = |x - x'|^2 + |x' - w|^2. \] (3.1.23)

This is because 
\[ x - x' = (x_n - \delta_n) \beta_n^*, \quad x' - w = x' - v - y \in U, \]
therefore,

\[(x - x') \perp (x' - w),\]

and (3.1.23) holds. Based on the assumption:

\[|x' - w|^2 \leq \frac{1}{4} (|\beta_1^*|^2 + \cdots + |\beta_{n-1}^*|^2).\]

It follows that

\[|x - w|^2 \leq \frac{1}{4} (|\beta_1^*|^2 + \cdots + |\beta_{n-1}^*|^2 + |\beta_n^*|^2) = \left(\frac{1}{2}\sigma(B)\right)^2.\]

Let \(x = t \in \mathbb{R}^n\), we get \(w \in L\) such that

\[|t - w| \leq \frac{1}{2}\sigma(B).\]

This lemma holds. \(\Box\)

The calculation of the covering radius on lattice is also a kind of hard problem. We define the covering radius problem (CDP\(_\gamma\)) based on parameter approximation.

**Definition 3.1.4** (CDP\(_\gamma\)) Let \(L\) be a full rank lattice, \(\gamma(n)\) be a parameter, CDP\(_\gamma\) problem is to find an \(r\) such that

\[\rho(L) \leq r \leq \gamma(n)\rho(L).\] (3.1.24)

### 3.2 SIS and Knapsack Problem on Ring

Let \(q\) be a positive integer, \(\mathbb{Z}_q\) be the residue class ring mod \(q\), and \(\mathbb{Z}_q[x]\) be the polynomial ring of one variable on \(\mathbb{Z}_q\). By (3.1.10), we define a quotient ring \(R_q\) on \(\mathbb{Z}_q[x]\)

\[R_q = \mathbb{Z}_q[x]/<x^n - 1> \cong (\mathbb{Z}_q^n, +, \otimes).\] (3.2.1)

To define the SIS problem on \(R_q\), for any \(m\) polynomials \(A = \{a_1(x), \ldots, a_m(x)\} \subset R_q\), \(A\) could be regarded as an \(m\) dimensional vector in \(R_q\), i.e. \(A = (a_1(x), \ldots, a_m(x)) \in R_q^n\), with the norm \(|A|\) defined by

\[|A| = \left(\sum_{i=1}^{m} |a_i(x)|^2\right)^{\frac{1}{2}} = \left(\sum_{i=1}^{m} |a_i|^2\right)^{\frac{1}{2}},\] (3.2.2)

where \(a_i(x) \longleftrightarrow a_i \in \mathbb{Z}_q^n\).
Definition 3.2.1 Let $\beta > 0$ be a positive real number, $n, m, q$ be positive integers. The SIS problem on $R_q$ is defined as follows: for any given uniformly distributed vector $A = (a_1(x), \ldots, a_m(x)) \in R_q^m$, find an $m$ dimensional vector $z = (z_1(x), z_2(x), \ldots, z_m(x)) \in R_q^m$ such that

\[
\begin{cases}
    f_A(z) = \sum_{i=1}^{m} a_i(x)z_i(x) = 0 \\
    0 < |z| = 
    \left( \sum_{i=1}^{m} |z_i(x)|^2 \right)^{\frac{1}{2}} \leq \beta.
\end{cases}
\] (3.2.3)

This problem is denoted as $R_q - \text{SIS}_{q,\beta,m}$.

Remark 3.2.1 By the above definition, $f_A(z) \in R_q$, so $f_A(z) = 0$ is equivalent to

\[
f_A(z) = \sum_{i=1}^{m} a_i(x)z_i(x) \equiv 0 \pmod{x^n - 1},
\]

here $0 < |z| \leq \beta$ is computed in the real number field $\mathbb{R}$.

Remark 3.2.2 In order to guarantee the $R_q - \text{SIS}_{q,\beta,m}$ problem has solution, we only need $m > \log_2 q$, which has big difference from the requirement $m > n \log q$ of the classical SIS problem (see Sect. 2.2 in the last chapter). In fact, if $A = (a_1(x), a_2(x), \ldots, a_m(x))$ is given, the selection of $z = (z_1(x), \ldots, z_m(x))$ could be considered in $\mathbb{Z}_q^n$. For each $z_i(x) \leftrightarrow z_i \in \mathbb{Z}_q^n$, choose each coordinate of $z_i$ as 0 or 1 so that the $n$ dimensional vector $z_i$ has a short length. There are about $2^n$ such short vectors $z_i$, so there are about $2^{mn}$ choices of $z$ in total. If $2^{mn} > q^n$, i.e. $mn > n \log_2 q$, $m > \log_2 q$, then $z' \in R_q^m, z'' \in R_q^m \Rightarrow$ 

\[
f_A(z') = f_A(z'') \Rightarrow f_A(z' - z'') = 0.
\]

So $z = z' - z''$ is the solution satisfying (3.2.3).

Geometric definition of $R_q - \text{SIS}_{q,\beta,m}$:

Given $m$ vectors $A = (a_1, a_2, \ldots, a_m)$ uniformly distributed on $\mathbb{Z}_q^n, a_i \in \mathbb{Z}_q^n$, solve a group of nonzero short vectors $z = (z_1, z_2, \ldots, z_m), z_i \in \mathbb{Z}_q^n$, such that

\[
\begin{cases}
    f_A(z) = \sum_{i=1}^{m} a_i \otimes z_i = 0 \\
    |z_i| \leq \sqrt{n}, \ 1 \leq i \leq n
\end{cases}
\] (3.2.4)

Obviously, $R_q - \text{SIS}$ problem is a special case of the knapsack problem on ring.
Definition 3.2.2 (Knapsack problem on ring) Let $R$ be a commutative ring with identity, $a_1, \ldots, a_m$ be $m$ nonzero elements in $R$, $X \subseteq R$, $|X| = 2^n$, $b \in R$ is called the target element. Knapsack problem on ring is to solve $m$ elements $z_1, z_2, \ldots, z_m \in X$ in $X$ such that
\[
f_A(z) = \sum_{i=1}^{m} a_i z_i = b, \ \forall z_i \in X.
\] (3.2.5)

If $R = \mathbb{Z}$ is a ring of integers, $X = \{0, 1\}$, or $X = \{0, 1, \ldots, 2^n - 1\}$, then the above problem is the classical knapsack problem. It has been proved that the computational complexity of solving the knapsack problem on $\mathbb{Z}$ is subexponential, such as the super increasing sequence is polynomial. If $R = \mathbb{R}^q$, $b = 0$, then the above problem becomes the SIS problem on $\mathbb{R}^q$. The main result in this section is the following theorem:

Theorem 3.2.1 Let $m = O(\log n)$, $k = \tilde{O}(\log n)$, $q \geq 4mkn^2$, and $\gamma \geq 16mkn^3$, if we can solve the knapsack problem (3.2.6) on $\mathbb{R}^q$, then there exists a probabilistic polynomial algorithm solving the covering radius problem $\text{CDP}_\gamma$ for any $n$ dimensional full rank cyclic lattice.

The knapsack problem on $\mathbb{R}^q$ in Theorem 3.2.1 is the more general case of (3.2.4), which is summarized in the following definition.

Knapsack problem on $\mathbb{R}^q$: Choose $m$ vectors $A = (a_1, a_2, \ldots, a_m)$ uniformly distributed on $\mathbb{Z}^n_q$ randomly and any target vector $b \in \mathbb{Z}^n_q$, find a set of short vectors $z = (z_1, z_2, \ldots, z_m)$ such that
\[
f_A(z) = \sum_{i=1}^{m} a_i \otimes z_i = b, \ |z_i| \leq \sqrt{n}, \ 1 \leq i \leq m.
\] (3.2.6)

From Theorem 3.2.1, the knapsack problem on $\mathbb{R}^q$ on the average case has a more difficult computational complexity than the covering radius problem on any full rank cyclic lattice under positive probability, which is another reduction principle from the worst case to the average case by Ajtai.

The core idea of the proof of Theorem 3.2.1 is to approximate the covering radius $\rho(L)$ of $L$ by $\frac{1}{2} \sigma(S)$ for any cyclic lattice $L = L(B) \subseteq \mathbb{R}^n$ under the assumption that (3.2.6) is solvable, where $S = \{s_1, s_2, \ldots, s_n\} \subseteq L$ is a set of $n$ linearly independent vectors, and
\[
\sigma(S) = \left( \sum_{i=1}^{n} |s_i^*|^2 \right)^{\frac{1}{2}}.
\]

\{s_1^*, s_2^*, \ldots, s_n^*\} is the corresponding orthogonal basis of $S$ using Gram-Schmidt algorithm. Since $|s_i^*| \leq |s_i|$ ($1 \leq i \leq n$), we have
\[ \sigma(S) = \left( \sum_{i=1}^{n} |s_i^*|^2 \right)^{\frac{1}{2}} \leq \left( \sum_{i=1}^{n} |s_i|^2 \right)^{\frac{1}{2}}. \] (3.2.7)

By Lemma 3.1.6, \( \rho(L) \leq \frac{1}{2} \sigma(S) \). The core steps of approximating \( \rho(L) \) by \( \frac{1}{2} \sigma(S) \) is summarized as follows.

**1) Reduced algorithm**

Randomly choose \( S = \{s_1, s_2, \ldots, s_n\} \subset L \) is a set of \( n \) linearly independent lattice vectors, assume that

\[ |S| = |s_n| = \max_{1 \leq i \leq n} |s_i|. \]

If \( \frac{1}{2} \sigma(S) \leq \gamma \rho(L) \), then the CDP\( \gamma \) problem on \( L \) is solved. If \( \sigma(S) > 2 \gamma \rho(L) \), we can find a lattice vector \( s' \in L \), such that

\[ |s'| \leq \frac{1}{2} |s_n| = \frac{1}{2} |S|, \]

and \( s_1, s_2, \ldots, s_{n-1}, s' \) are linearly independent. Replace \( S \) with the new set of vectors \( S' = \{s_1, s_2, \ldots, s_{n-1}, s'\} \), that is, replace \( s_n \) with \( s' \) in \( S \). Repeat this process \( n \) times and we can get

\[ |S'| \leq \frac{1}{2} |S|. \] (3.2.8)

Repeat the above reduced algorithm, and find a set of linearly independent vectors \( S \subset L \), such that

\[ |S| \leq \frac{2 \gamma}{\sqrt{n}} \rho(L), \] (3.2.9)

and the computational complexity of the algorithm is polynomial. Based on (3.2.9), we have

\[ \rho(L) \leq \frac{1}{2} \sigma(S) \leq \frac{\sqrt{n}}{2} |S| \leq \gamma \rho(L). \]

So we complete solving the CDP\( \gamma \) problem.

**2) Approximation of standard orthogonal basis**

Let \( \{e_0, e_1, \ldots, e_{n-1}\} \subset \mathbb{Z}^n_q \) be a standard orthogonal basis, \( L = L(B) \subset \mathbb{R}^n \) be a given cyclic lattice. Define the parameter

\[ \beta = \left( \frac{4nq}{\gamma} + \frac{\sqrt{n}}{2} \right) \sigma(S), \] (3.2.10)

where \( S = \{s_1, s_2, \ldots, s_n\} \subset L \) is a set of \( n \) linearly independent vectors, such that

\[ \sigma(S) > 2 \gamma \rho(L). \] (3.2.11)
To find \( s' \) in the reduced algorithm, by Lemma 3.1.6, there is a lattice vector \( c \in L \Rightarrow \)

\[
|c - \beta e_0| \leq \frac{1}{2} \sigma(S). \tag{3.2.12}
\]

Since \( T \) is an orthogonal matrix, it is an orthogonal linear transformation in \( \mathbb{R}^n \), i.e.

\[
|T\alpha| = |\alpha|, \ \forall \alpha \in \mathbb{R}^n.
\]

Therefore, for any \( 0 \leq k \leq n - 1 \),

\[
|T^k(c - \beta e_0)| = |c - \beta e_0| \leq \frac{1}{2} \sigma(S).
\]

Note that \( T^k e_0 = e_k \), so

\[
|T^k c - \beta e_k| \leq \frac{1}{2} \sigma(S).
\]

Because \( c \in L \) and \( L \) is a cyclic lattice, then \( T^k c \in L \) \( (0 \leq k \leq n - 1) \). The circulant matrix \( T^*(c) = [c, Tc, \ldots, T^{k-1}c] \) implements the approximation of standard orthogonal basis.

In order to give a complete proof of theorem 3.2.1, we denote

\[
B' = q(T^*(c))^{-1}B. \tag{3.2.13}
\]

**Lemma 3.2.1** The lattice \( L(B') \) generated by \( B' \) satisfies \( q\mathbb{Z}^n \subset L(B') \).

**Proof** By Lemma 3.1.5, since \( c \in L \) and \( L \) is a cyclic lattice, there exists an integer matrix \( D \in \mathbb{Z}^{n \times n} \) such that

\[
T^*(c) = BD \Rightarrow B^{-1}T^*(c) \in \mathbb{Z}^{n \times n}.
\]

thus,

\[
B'(B^{-1}T^*(c)) = q(T^*(c))^{-1} \cdot B \cdot B^{-1}T^*(c) = qI_n.
\]

Each column of the above matrix \( qe_j \) \( (0 \leq j \leq n - 1) \) \( \in L(B') \Rightarrow q\mathbb{Z}^n \subset L(B') \). \( \square \)

Based on Lemma 3.2.1, \( q\mathbb{Z}^n \) is an additive subgroup in \( L(B') \). Randomly choose \( mk \) vectors \( x_{ij}^j \in G \) \( (1 \leq i \leq m, 1 \leq j \leq k) \) in the quotient group \( G = L(B')/q\mathbb{Z}^n \), the integral vectors \( w_{ij}' \) of \( x_{ij}' \) is defined by

\[
w_{ij}' = [x_{ij}'] \in \mathbb{Z}^n, \ 1 \leq i \leq m, \ 1 \leq j \leq k.
\]

Let

\[
a_i \equiv \sum_{j=1}^k w_{ij}' \text{ (mod } q) \Rightarrow a_i \in \mathbb{Z}_q^n, \tag{3.2.14}
\]
$A = (a_1, a_2, \ldots, a_m)$ contains the above $m$ vectors in $\mathbb{Z}_n^q$, consider the knapsack problem on $R_q = (\mathbb{Z}_n^q, +, \otimes)$,

$$f_A(z) = \sum_{i=1}^{m} a_i \otimes z_i, \forall z_i \in \mathbb{Z}_n^q, |z_i| \leq \sqrt{n}.$$ 

If we can solve the knapsack problem on $R_q$, then $f_A(z)$ collision is also solvable. So there are integral vectors $y = (y_1, y_2, \ldots, y_m)$, $\hat{y} = (\hat{y}_1, \hat{y}_2, \ldots, \hat{y}_m)$ such that

$$f_A(y - \hat{y}) = \sum_{i=1}^{m} a_i \otimes (y_i - \hat{y}_i) = 0, \forall |y_i| \leq \sqrt{n}, |\hat{y}_i| \leq \sqrt{n}, \quad (3.2.15)$$

where

$$y = (y_1, y_2, \ldots, y_m), \hat{y} = (\hat{y}_1, \hat{y}_2, \ldots, \hat{y}_m). \quad (3.2.16)$$

Based on the vector clusters $y$ and $\hat{y}$ in $\mathbb{Z}_n^q$, we define

$$s' = \sum_{i=1}^{m} \sum_{j=1}^{k} (x_{ij} - w_{ij}) \otimes (y_i - \hat{y}_i). \quad (3.2.17)$$

The $s'$ defined by the above formula is just the $s'$ in the reduced algorithm. First, we prove the following lemma.

**Lemma 3.2.2** $x_{ij} \in L(B)$ is a lattice vector in the given cyclic lattice $L (1 \leq i \leq m, 1 \leq j \leq k)$, and if $f_A(y) = f_A(\hat{y})$, $s' \in L(B)$ is also a lattice vector.

**Proof** Since $x'_{ij} \in L(B')$, there is $\alpha \in \mathbb{Z}^n$ such that $x'_{ij} = B'\alpha$, we get

$$x_{ij} = \frac{1}{q} T^*(c) x'_{ij} \quad \text{and} \quad w_{ij} = \frac{1}{q} T^*(c) w'_{ij}.$$ 

To prove $s' \in L(B)$, by (3.2.17) and the property of circulant matrix (see (3.1.5))

$$s' = \sum_{i=1}^{m} \sum_{j=1}^{k} (y_{ij} - \hat{y}_{ij}) - \sum_{i=1}^{m} \sum_{j=1}^{k} (y_{ij} - \hat{y}_{ij})$$

$$= \sum_{i=1}^{m} T^*(1) (y_{ij} - \hat{y}_{ij}) - \sum_{i=1}^{m} T^*(1) (y_{ij} - \hat{y}_{ij})$$

$$= \sum_{i=1}^{m} T^*(1) (y_{ij} - \hat{y}_{ij}) - \sum_{j=1}^{k} T^*(1) (y_{ij} - \hat{y}_{ij}). \quad (3.2.18)$$
Based on the first conclusion, $x_{ij} \in L(B) \Rightarrow \sum_{j=1}^{k} x_{ij} \in L(B)$, since $y_i$ and $\hat{y}_i$ are integral vectors in $\mathbb{Z}_q^n$, it follows that

$$T^* \left( \sum_{j=1}^{k} x_{ij} \right) (y_i - \hat{y}_i) \in L(B).$$

Next we prove the second term of (3.2.18) is also a lattice vector. By the definition of $w_{ij}$,

$w_{ij} = \frac{1}{q} T^*(c) w'_{ij}$, then $\sum_{j=1}^{k} w_{ij} = \frac{1}{q} T^*(c) \left( \sum_{j=1}^{k} w'_{ij} \right)$.

Hence,

$$T^* \left( \sum_{j=1}^{k} w_{ij} \right) = \frac{1}{q} T^*(c) T^* \left( \sum_{j=1}^{k} w'_{ij} \right).$$

The second term of (3.2.18) could be written as

$$\sum_{i=1}^{m} T^* \left( \sum_{j=1}^{k} w_{ij} \right) (y_i - \hat{y}_i) = \frac{1}{q} T^*(c) \sum_{i=1}^{m} T^* \left( \sum_{j=1}^{k} w'_{ij} \right) (y_i - \hat{y}_i)$$

$$= \frac{1}{q} T^*(c) \sum_{i=1}^{m} \sum_{j=1}^{k} w'_{ij} \otimes (y_i - \hat{y}_i).$$

(3.2.19)

Since

$$\sum_{i=1}^{m} \sum_{j=1}^{k} w'_{ij} \otimes (y_i - \hat{y}_i) \equiv \sum_{i=1}^{m} a_i \otimes (y_i - \hat{y}_i) \pmod{q} \equiv f_A(y) - f_A(\hat{y}) \pmod{q},$$

by $f_A(y) = f_A(\hat{y})$, we know the second term of (3.2.18) is in $L(B)$, i.e.

$$\sum_{i=1}^{m} T^* \left( \sum_{j=1}^{k} w_{ij} \right) (y_i - \hat{y}_i) \in L(B).$$

Finally we have $s' \in L(B)$ based on (3.2.18).

□

**Lemma 3.2.3** The lattice vector $s'$ defined in (3.2.17) satisfies

$$|s'| \leq \frac{1}{2} |s_n| = \frac{1}{2} |S|. \quad (3.2.20)$$
Proof We only prove $|s'| \leq \sigma(S)/2\sqrt{n}$, since

$$\sigma(S) \leq \left( \sum_{i=1}^{n} |s_i|^2 \right)^{\frac{1}{2}} \leq \sqrt{n}|S| = \sqrt{n}|s_n|,$$

we can get $|s'| \leq \frac{1}{2}|s_n|$, and the lemma is proved. Based on the definition of $s'$,

$$|s'| \leq \sum_{i=1}^{m} \sum_{j=1}^{k} |(x_{ij} - w_{ij}) \otimes (y_{ij} - \hat{y}_{ij})|.$$  \tag{3.2.21}

It follows that

$$x_{ij} - w_{ij} = \frac{1}{q} T^*(c)(x_{ij} - w_{ij}) = \frac{1}{q} c \otimes (x_{ij} - w_{ij}).$$

Let $\alpha = c - \beta e_0$, then $|\alpha| \leq \frac{1}{2} \sigma(S)$ (see (3.2.12)), and

$$x_{ij} - w_{ij} = \frac{1}{q} (\alpha + \beta e_0) \otimes (x_{ij} - w_{ij}) = \frac{1}{q} T^*(\alpha + \beta e_0)(x_{ij} - w_{ij})$$

$$= \frac{1}{q} \beta T^*(e_0)(x_{ij} - w_{ij}) + \frac{1}{q} T^*(\alpha)(x_{ij} - w_{ij})$$

$$= \frac{\beta}{q} (x_{ij} - w_{ij}) + \frac{1}{q} T^*(\alpha)(x_{ij} - w_{ij}).$$

Since

$$|x_{ij} - w_{ij}| \leq \frac{1}{2} \sqrt{n},$$

combine with (3.1.15) in the last section, we have ($\beta$ is determined by (3.2.10))

$$|x_{ij} - w_{ij}| \leq \frac{\beta}{q} |x_{ij} - w_{ij}| + \frac{1}{q} |\alpha \otimes (x_{ij} - w_{ij})|$$

$$\leq \frac{\beta}{q} \cdot \frac{1}{2} \sqrt{n} + \frac{1}{q} \cdot \frac{\sqrt{n}}{2} \cdot \sqrt{n} \cdot \frac{1}{2} \sigma(S)$$

$$= \frac{\beta}{q} \cdot \frac{\sqrt{n}}{2} + \frac{1}{q} \cdot \frac{\sqrt{n}}{2} \cdot \frac{\sigma(S)}{\gamma} \cdot \frac{\sqrt{n}}{2}$$

$$= \sigma(S) \left( \frac{2n^2}{\gamma} + \frac{n}{2q} \right)$$

$$\leq \sigma(S) \left( \frac{1}{8} \cdot \frac{1}{mkn^2} + \frac{1}{8} \cdot \frac{1}{mkn^2} \right)$$

$$= \frac{1}{4} \sigma(S) \frac{1}{mkn^2}.$$
Based on (3.2.21), we get

$$|s'| \leq m k \sqrt{n} \max_{i,j} |x_{ij} - w_{ij}| \cdot \max_{i} |y_{i} - \hat{y}_{i}|$$

$$\leq m k \sqrt{n} \cdot 2 \sqrt{n} \max_{i,j} |x_{ij} - w_{ij}| \leq \frac{\sigma(S)}{2 \sqrt{n}}.$$ 

So we complete the proof of Lemma 3.2.3. □

From the above lemma, the reduced algorithm required in Theorem 3.2.1 is proved. However, we must prove that \(\{a_i\}_{i=1}^{m} \subset \mathbb{Z}_{q}^{n}\) determined by (3.2.14) is uniformly distributed, so that the knapsack problem on \(R_q\) is solved in the average case. Next we prove that \(\{a_i\}_{i=1}^{m}\) is almost uniformly distributed in \(\mathbb{Z}_{q}^{n}\), that is, the statistical distance between the distribution of \(\{a_i\}\) and the uniform distribution is sufficiently small. We first prove the following lemma.

**Lemma 3.2.4** Let \(B' = q(T^*(c))^{-1} B\), then the covering radius \(\rho(B')\) of \(L(B')\) satisfies

$$\rho(B') \leq \frac{1}{8n},$$

where \(L(B)\) is a full rank cyclic lattice, \(c \in L(B)\) is given by (3.2.12).

**Proof** Based on the definition of covering radius,

$$\rho(B') = \max_{x \in \mathbb{R}^n} |x - u_x| = \max_{x \in \mathbb{R}^n} |x - L(B')|.$$ 

Let \(t' \in \mathbb{R}^n\) be the vector achieving the maximum value above, i.e. \(|t' - L(B')| \geq \rho(B')\), and

$$|t' - B'z| \geq \rho(B'), \quad \forall z \in \mathbb{Z}^n.$$ 

Denote

$$t = \frac{1}{q} T^*(c)t'.$$

Suppose \(Bz_0 \in L(B)\) is the nearest lattice vector of \(t\), then we have

$$\rho(B) \geq \text{dist}(t, L(B)) = |t - Bz_0|$$

$$= \frac{1}{q} T^*(c)t' - Bz_0 = \frac{1}{q} T^*(c)(t' - B'z_0)$$

$$\geq \frac{1}{q} |t' - B'z_0| \min_{d \in \mathbb{R}^n, d \neq 0} \frac{|c \otimes d|}{|d|}$$

$$\geq \frac{1}{q} \rho(B') \min_{d \in \mathbb{R}^n, d \neq 0} \frac{|c \otimes d|}{|d|}. \quad (3.2.22)$$
For any \(d \in \mathbb{R}^n, d \neq 0\), we estimate the value of \(c \otimes d\). Since \(c = \beta e_0 + \alpha\), where \(|\alpha| \leq \frac{1}{2^2} \sigma(S)\), so
\[
|c \otimes d| = |(\beta e_0 + \alpha) \otimes d| \\
\geq |d| (\beta - \frac{1}{2} \sqrt{n} \sigma(S)) \\
\geq \beta |d| - \sqrt{n} |\alpha||d| \\
= |d| \frac{4nq}{\gamma} \sigma(S).
\]

By (3.2.22), we have (see (3.2.11))
\[
\rho(B) \geq \frac{1}{q} \rho(B') \cdot \frac{4nq}{\gamma} \sigma(S) \\
\geq 8n \rho(B') \rho(B).
\]

This implies \(\rho(B') \leq \frac{1}{8n}\). Lemma 3.2.4 holds. \(\square\)

**Lemma 3.2.5** Let \(\Lambda = L(B)\) be a lattice, \(Q \subset \mathbb{R}^n\) is convex and contains a ball with the radius \(r \geq \rho(\Lambda)\). Then the number of lattice vectors of \(L(B)\) contained in \(Q\) satisfies
\[
\frac{\text{Vol}(Q)}{\det(\Lambda)} (1 - \frac{\rho(\Lambda)n}{\gamma}) \leq |L(B) \cap Q| \leq \frac{\text{Vol}(Q)}{\det(\Lambda)} (1 + \frac{2\rho(\Lambda)n}{\gamma}).
\]

**Proof** See Lyubashevsky and Micciancio (2006) or Lyubashevsky (2010).

Based on the above lemma, let \(\Lambda = L(B')\), we estimate the distribution of vectors \(\{a_{ij}\}\) in \(\mathbb{Z}_q^n\). From the definition
\[
a_{ij} \equiv w_{ij}' \pmod{q}, \quad a_i \equiv \sum_{j=1}^k a_{ij} \pmod{q}, \quad (3.2.23)
\]
where \(w_{ij}'\) is the rounding vector of \(x_{ij}' \in G = L(B')/q\mathbb{Z}^n\). The ball taking \(w_{ij}'\) as the center with radius \(\frac{1}{2}\) is contained in the cube centered as \(w_{ij}'\) with the side length \(\frac{1}{2}\). Since \(\rho(L(B')) \leq \frac{1}{8q} < \frac{1}{2}\), from lemma 3.2.4, the number \(N\) of lattice vectors of \(L(B')\) in this cube satisfies
\[
\frac{1}{\det(B')} \left(1 - \frac{1}{4}\right) \leq N \leq \frac{1}{\det(B')} (1 + \frac{1}{2}).
\]

For any \(a \in R_q = \mathbb{Z}_q^n\), because \(x_{ij}'\) is uniformly selected in \(L(B')/q\mathbb{Z}^n\), there are
\[
|L(B')/q\mathbb{Z}^n|^{-1} = \frac{q^n}{\det(B')}
\]
possible choices, therefore,

\[
\left| \Pr[a_{ij} = a] - \frac{1}{q^n} \right| \leq \frac{1}{2q^n}. \tag{3.2.24}
\]

Now we estimate the probability distribution of \( \{a_i\}_{i=1}^m \).

**Lemma 3.2.6** Let \( G \) be a finite Abel group, \( A_1, A_2, \ldots, A_k \) be \( k \) independent random variables on \( G \), such that for any element \( x \in G \),

\[
\left| \Pr[A_i = x] - \frac{1}{|G|} \right| \leq \frac{1}{2|G|}.
\]

Then the statistical distance between \( \xi = \sum_{i=1}^k A_i \) and the uniform distribution on \( G \) is

\[
\Delta(\xi, U(G)) \leq 2^{-(k+1)}.
\]

**Proof** We use mathematical induction to prove that the following inequality holds for any positive integer \( k \),

\[
\left| \Pr[\xi = x] - \frac{1}{|G|} \right| \leq \frac{1}{2^k|G|}, \forall x \in G.
\]

If \( k = 1 \), the inequality above holds. Assume it holds for \( k - 1 \), denote \( \xi' = \sum_{i=1}^{k-1} A_i \), \( \xi = \xi' + A_k \), we have

\[
\left| \Pr[\xi = x] - \frac{1}{|G|} \right| = \sum_{a \in G} \Pr[\xi' = a, A_k = x - a] - \frac{1}{|G|} \\
= \sum_{a \in G} \Pr[\xi' = a] \Pr[A_k = x - a] - \frac{1}{|G|} \\
= \sum_{a \in G} \left( \Pr[\xi' = a] - \frac{1}{|G|} \right) \left( \Pr[A_k = x - a] - \frac{1}{|G|} \right) \\
\leq \sum_{a \in G} \frac{1}{2^{k-1}|G|} \cdot \frac{1}{2|G|} = \frac{1}{2^k|G|}.
\]

Thus,

\[
\Delta(\xi, U(G)) = \frac{1}{2} \sum_{x \in G} \left| \Pr[\xi = x] - \frac{1}{|G|} \right| \leq \frac{1}{2} \sum_{x \in G} \frac{1}{2^k|G|} = 2^{-(k+1)}.
\]

This lemma holds. \( \square \)
From (3.2.23), (3.2.24) and Lemma 3.2.5, we know that each \( a_i = \sum_{j=1}^{k} a_{ij} \) is almost uniformly distributed on \( \mathbb{Z}_q^n \), i.e. the statistical distance between \( a_i \) and the uniform distribution is sufficiently small. Therefore, the knapsack problem on \( R_q \) sampled by \( f_A(z) \) is in the average case. So far, we have completed the proof of Theorem 3.2.1.

### 3.3 LWE Problem

The LWE problem is to solve a kind of random linear equations under a given probability distribution. To better understand the LWE problem, let’s start with the checking learning problem (LPE) with errors. Let \( \mathbb{Z}_2 = \{0, 1\} \) be a finite field with 2 elements, \( n \geq 1 \) and \( \varepsilon \geq 0 \) be a given parameter. The distribution of \( \xi \) with parameter \( \varepsilon \) on \( \mathbb{Z}_2 \) is

\[
\Pr\{\xi = 0\} = 1 - \varepsilon, \quad \Pr\{\xi = 1\} = \varepsilon.
\]

If \( a, b \in \mathbb{Z}_2 \), the probability that \( a \) and \( b \) having the same parity is \( 1 - \varepsilon \), i.e.

\[
\Pr\{a \equiv b \pmod{2}\} = 1 - \varepsilon,
\]

denoted as \( a \equiv_{\varepsilon} b \). The checking learning problem with errors LPE is: given \( m \) independent vectors \( \{a_1, a_2, \ldots, a_m\} \), \( a_i \in \mathbb{Z}_2^n \) uniformly distributed on \( \mathbb{Z}_2^n \), and \( b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{Z}_2^m \), to solve a vector \( s \in \mathbb{Z}_2^n \), such that the following \( m \) random congruence equations hold simultaneously

\[
\begin{align*}
  b_1 &\equiv_{\varepsilon} <a_1, s> \pmod{2} \\
  b_2 &\equiv_{\varepsilon} <a_2, s> \pmod{2} \\
  \vdots &
\end{align*}
\]

(3.3.1)

where \( <a_i, s> \) is the inner product of two vectors in \( \mathbb{Z}_2^n \). If \( \varepsilon = 0 \), then the distribution \( \xi \) becomes the trivial distribution, and (3.3.1) becomes \( m \) deterministic congruence equations. At this time, the LPE problem could be solved by Gauss elimination method with only \( n \) equations, and the computational complexity is a polynomial of \( n \). If \( \varepsilon > 0 \), the LPE problem is nontrivial, and its computational complexity is exponential of \( n \). For example, the likelihood algorithm requires \( O(n) \) random congruence equations with computational complexity \( 2^{O(n)} \). In 2003, Blum et al. (2003) proposed a subexponential algorithm whose computational complexity and the number of random congruence equations are both \( 2^{O(n/\log n)} \), which is the best result of the LPE question so far.
Generalizing the LPE problem from mod 2 to the general case mod \(q\), it becomes the LWE problem. Due to the important role of the LWE problem in modern anti-quantum computing cryptosystems, we will introduce the related concepts and results in detail in this section. First, we define the random congruence equation with error on the integer ring \(\mathbb{Z}\). Let \(n \geq 1\), \(q \geq 2\) be two positive integers, \(\mathbb{Z}_q\) be the residue class ring of mod \(q\), and \(\chi\) be a probability distribution on \(\mathbb{Z}_q\).

**Definition 3.3.1** Let \(a, b \in \mathbb{Z}, e \in \mathbb{Z}_q\), if

\[
\Pr[a \equiv b + e \pmod{q}] = \chi(e),
\]

we call \(a\) and \(b\) are congruential mod \(q\) under the distribution \(\chi\), denoted as

\[
a \equiv_{\chi} b + e \pmod{q}, \text{ or } a =_{\chi} b + e.
\]

The above formula is called a random congruence equation with error under \(\chi\), and it is abbreviated as \(a = b + e\) sometimes.

Based on the above random congruence equation, we give the definition of the LWE distribution \(A_{s,\chi}\).

**Definition 3.3.2** Let \(s \in \mathbb{Z}_q^n\), \(\chi\) be a given distribution on \(\mathbb{Z}_q\), the LWE distribution \(A_{s,\chi} = (a, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q\) generated by \(s\) and \(\chi\) satisfies:

1. \(a \in \mathbb{Z}_q^n\) is uniformly distributed;
2. \(b =_{\chi} < a, s > + e\), where \(< a, s >\) is the inner product of \(a\) and \(s\) in \(\mathbb{Z}_q\), \(e \in \mathbb{Z}_q\) has the distribution \(\chi\), i.e. \(e \leftarrow \chi\). We call \(A_{s,\chi} = (a, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q\) the LWE distribution, \(s\) is called the private key and \(e\) is called the error distribution. If \(b \in \mathbb{Z}_q\) is uniformly distributed, then \(A_{s,\chi}\) is called the uniform LWE distribution.

Under the LWE distribution \(A_{s,\chi} = (a, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q\), for a given error \(e \in \mathbb{Z}_q\), the essence of finding the private key \(s = (s_1, s_2, \ldots, s_n)' \in \mathbb{Z}_q^n\) is solving the random knapsack problem on the ring \(\mathbb{Z}_q\):

\[
b \equiv a_1s_1 + a_2s_2 + \cdots + a_ns_n \pmod{q},
\]

solve \(s \in \mathbb{Z}_q^n\) under the probability distribution \(\chi(e)\). Next, we give the definition of LWE problem \(\text{LWE}_{n,q,\chi,m}\) with the parameters \(n \geq 1\), \(q \geq 2\), \(m \geq 1\) and \(\chi\).

**Definition 3.3.3** For any \(m\) independent samples \((a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q\) \((1 \leq i \leq m)\) of \(A_{s,\chi}\), and randomly selected samples of the error distribution \(e = \begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix}\), \(e_i \in \mathbb{Z}_q\),
Learning with Error

\( \mathbb{Z}_q, e_i \leftarrow \chi \), the LWE\(_{n,q,\chi,m} \) problem is to solve the private key \( s \in \mathbb{Z}_q^n \) with high probability (larger than \( 1 - \delta \)). In other words, solve \( s \in \mathbb{Z}_q^n \) satisfying

\[
\begin{align*}
& b_1 = \chi < a_1, s > + e_1 \\
& b_2 = \chi < a_2, s > + e_2 \\
& \vdots \\
& b_m = \chi < a_m, s > + e_m \\
\end{align*}
\]  
(3.3.4)

**Remark 3.3.1** If \( \chi \) is the trivial distribution, i.e. \( \chi(0) = 1, \chi(k) = 0 \) for \( 1 \leq k < q \), then the samples of \( \chi \) are \( e = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \), (3.4) becomes \( m \) deterministic congruence equations

\[
\begin{align*}
& b_1 \equiv a_1, s > \pmod{q} \\
& b_2 \equiv a_2, s > \pmod{q} \\
& \vdots \\
& b_m \equiv a_m, s > \pmod{q} \\
\end{align*}
\]

Based on the Gauss elimination, we can calculate the only private key \( s \in \mathbb{Z}_q^n \) from \( n \) congruence equations, and the computational complexity is polynomial.

**Remark 3.3.2** Let \( q = 2 \), \( \chi \) be the two point distribution with parameter \( \varepsilon \) on \( \mathbb{Z}_2 \), then the LWE problem on \( \mathbb{Z}_2 \) is just the LPE problem. For any error distribution \( e = \begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix} \), if \( e_i = 1 \), from

\[
\Pr\{ b_i \equiv a_i, s > +1 \pmod{2} \} = \varepsilon,
\]

we can get

\[
\Pr\{ b_i \equiv a_i, s > \pmod{2} \} = 1 - \varepsilon.
\]

**Matrix representation of the LWE\(_{n,q,\chi,m} \) problem**

Let \( A = [a_1, a_2, \ldots, a_m]_{n \times m} \in \mathbb{Z}_q^{n \times m} \) be a random matrix uniformly distributed, \( b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{Z}_q^m \), \( e = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix} \in \mathbb{Z}_q^m \) be the errors, and \( e \leftarrow \chi^m \), solve the private key \( s \in \mathbb{Z}_q^n \), such that

\[
b \equiv \chi A^\prime s + e \pmod{q}, \tag{3.3.5}
\]

where \( A^\prime \) is the transpose matrix of \( A \), and (3.3.5) is a set of random congruence equations with errors. The probability that the \( i \)th congruence equation holds is
3.3 LWE Problem

Let \( \chi(e_i) \), so
\[
\Pr\{b \equiv \chi A's + e \pmod{q}\} = \prod_{i=1}^{m} \chi(e_i) = \chi(e).
\] (3.3.6)

Let \( \Lambda_q(A) \) and \( \Lambda_q^\perp(A) \) be \( q \) ary integral lattices (see Sect. 7.3 of Chap. 7 in Zheng (2022)), defined by:
\[
\left\{ \begin{array}{l}
\Lambda_q(A) = \{ Ax \mid x \in \mathbb{Z}_q^n \} + q\mathbb{Z}_q^n \\
\Lambda_q^\perp(A) = \{ x \in \mathbb{Z}_q^m \mid Ax \equiv 0 \pmod{q} \}
\end{array} \right. \] (3.3.7)

Since \( \Lambda_q(A) = q \Lambda_q^\perp(A)^\ast \), \( A's \in \Lambda_q(A) \), the geometric meaning of LWE \( n, q, \chi, m \) is to solve a lattice vector \( A's \) near from \( b \) for any \( b \in \mathbb{Z}_q^m \), such that the distance \( b - A's \) has the distribution \( \chi^m \), which is dual to the SIS problem.

**Lemma 3.3.1** Suppose \( A \in \mathbb{Z}_q^{n \times m} \) is a random matrix uniformly distributed, \( A = [A_1, A_2] \), where \( A_1 \in \mathbb{Z}_q^{n \times n} \) is an invertible matrix, let \( \overline{A} = A_1^{-1}A = [I_n, A_1^{-1}A_2] \), then \( A_{s,\chi} \) and \( \overline{A}_{s,\chi} \) have the same probability distribution.

**Proof** From Lemma 2.1.1 in Chap. 2, if \( A \) is uniformly distributed, then \( \overline{A} \) is also a uniform random matrix. Assume \( b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \), \( e = \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} \), \( s \in \mathbb{Z}_q^n \) satisfy
\[
b \equiv \chi A's + e \pmod{q},
\]
that is,
\[
\left\{ \begin{array}{l}
b_1 \equiv \chi A_1's + e_1 \pmod{q} \\
b_2 \equiv \chi A_2's + e_2 \pmod{q}
\end{array} \right. .
\]
Let \( A_1^* = (A_1')^{-1} \), and
\[
\overline{b} = \begin{pmatrix} A_1^*b_1 \\ A_1^*b_2 \end{pmatrix} , \quad \overline{e} = \begin{pmatrix} A_1^*e_1 \\ A_1^*e_2 \end{pmatrix} .
\]

Obviously, \( \overline{b} \) and \( b \) have the same probability distribution, so are \( \overline{e} \) and \( e \),
\[
\overline{b} \equiv \chi A_1^* \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \pmod{q} \equiv \chi A_1^*(A's + e) \pmod{q}
\]
\[
\equiv \chi A_1^*A's + A_1^*e \pmod{q} \equiv \chi \overline{A}s + e \pmod{q}.
\]
The lemma holds. \( \square \)

The above \( \overline{A} = [I_n, A_1^{-1}A_2] \) is called the normal form of the LWE problem.

**Lemma 3.3.2** Let \( x, y, z \) be three random variables on \( \mathbb{Z}_q \), \( x \) and \( y \) are independent, \( z \equiv x + y \pmod{q} \). If \( x \) is uniformly distributed on \( \mathbb{Z}_q \), so is \( z \).
Proof For any integer $0 \leq i \leq q - 1$, we compute the probability that $z$ takes the value $i$.

$$\Pr\{z = i\} = \sum_{j=0}^{q-1} \Pr\{x = j, y = i - j\}$$

$$= \sum_{j=0}^{q-1} \Pr\{x = j\} \Pr\{y = i - j\}$$

$$= \frac{1}{q} \sum_{j=0}^{q-1} \Pr\{y = i - j\} = \frac{1}{q}.$$

Lemma 3.3.3 In the LWE distribution $A_{s, \chi} = (a, b)$, $b$ is uniformly distributed if and only if $b - <a, s>$ is uniformly distributed.

Proof If $b - <a, s>$ is uniformly distributed, from $b = (b - <a, s>)+ <a, s>$ and Lemma 3.3.2, we get $b$ is uniform. On the other hand, if $b$ is uniform, from $b - <a, s> = b + (-<a, s>)$ and Lemma 3.3.2 again, $b - <a, s>$ is also uniformly distributed. □

According to Definition 3.3.1, the above lemma gives an equivalent condition that $A_{s, \chi}$ is a uniform LWE distribution. An equivalent form of the LWE problem is the decision LWE problem, which we call the D-LWE problem.

Definition 3.3.4 (D-LWE problem) Given $a \in \mathbb{Z}_q^n$ is uniformly distributed, $s \in \mathbb{Z}_q^n$, $e \in \mathbb{Z}_q$ with the distribution $\chi$, decide whether $<a, s> + e$ is uniform under positive probability of $s$.

The D-LWE problem seems easy, however, the difficulty of it is equivalent to that of the LWE problem. We will prove this equivalence in detail in Sect. 3.4. Here we focus on the probability distribution $\chi$ of the LWE problem. Usually, $\chi$ takes the discrete Gauss distribution on $\mathbb{Z}_q$. In Chapter 1, we discussed the discretization of continuous random variable with Gauss distribution in $\mathbb{R}^n$ on lattice in detail. The discrete Gauss distribution on $\mathbb{Z}_q$ is actually the discretization of Gauss distribution on $\mathbb{Z}_q$.

Recall the definition of Gauss function $\rho_s(x)$ in Chap. 1 (see (3.2.1),

$$\rho_s(x) = e^{-\frac{s}{2}|x|^2}, \ x \in \mathbb{R}^n. \quad (3.3.8)$$

If $n = 1$, $\rho_s(x)$ is a density function of continuous random variable on $\mathbb{R}$. We convert the corresponding random variable of $\rho_s(x)$ to mod 1, which becomes a continuous random variable defined on $\mathbb{T} \equiv [0, 1)$ (mod 1) of length 1, with the density function
\[ \psi_{\beta}(x) = \sum_{k=-\infty}^{+\infty} \frac{1}{\beta} e^{-\frac{\pi}{\beta^2}(x-k)^2}, \quad x \in \mathbb{T}. \quad (3.3.9) \]

It is easy to see that

\[ \int_{\mathbb{T}} \psi_{\beta}(x) \, dx = \int_{0}^{1} \psi_{\beta}(x) \, dx = \int_{\mathbb{R}} \frac{1}{\beta} \rho_{\beta}(x) \, dx = 1. \]

In order to estimate the statistical distance between random variables defined by different \( \beta \), we first prove the following two lemmas.

**Lemma 3.3.4** Let \( t \) and \( l \) be positive real numbers, \( x, \ y \in \mathbb{R}^n \) satisfy

\[ |x| \leq t, \text{ and } |x - y| \leq l. \]

Then

\[ \rho_s(y) \geq \left( 1 - \frac{\pi}{s^2} (2tl + l^2) \right) \rho_s(x). \quad (3.3.10) \]

**Proof** For any \( z \in \mathbb{R} \), we have

\[ e^{-z} \geq 1 - z, \quad z \in \mathbb{R}. \]

Therefore,

\[ \rho_s(y) = e^{-\frac{\pi}{s^2} |y|^2} \geq e^{-\frac{\pi}{s^2} (|x|+|y-x|)^2} \]
\[ \geq e^{-\frac{\pi}{s^2} (|x|^2+2|x||y-x|+l^2)} \]
\[ \geq e^{-\frac{\pi}{s^2} (|x|^2+2tl+l^2)} \]
\[ \geq (1 - \frac{\pi}{s^2} (2tl + l^2)) \rho_s(x). \]

\[ \square \]

**Lemma 3.3.5** Let \( 0 < \alpha < \beta \leq 2\alpha \), then the statistical distance between \( \psi_{\alpha} \) and \( \psi_{\beta} \) satisfies

\[ \Delta(\psi_{\alpha}, \psi_{\beta}) \leq \frac{9}{2} \left( \frac{\beta}{\alpha} - 1 \right). \quad (3.3.11) \]

**Proof** Based on

\[ \int_{0}^{1} \psi_{\beta}(x) \, dx = 1, \]

it follows that
\[
\int_0^1 |\psi_\beta(x) - \psi_\alpha(x)| \, dx \\
= \int_0^1 \left| \sum_{k=-\infty}^{+\infty} \left( \frac{1}{\beta} e^{-\frac{\pi}{\beta^2} |k-x|^2} - \frac{1}{\alpha} e^{-\frac{\pi}{\alpha^2} |k-x|^2} \right) \right| \, dx \\
\leq \sum_{k=-\infty}^{+\infty} \int_0^1 \left| \frac{1}{\beta} e^{-\frac{\pi}{\beta^2} |x-k|^2} - \frac{1}{\alpha} e^{-\frac{\pi}{\alpha^2} |x-k|^2} \right| \, dx \\
= \int_{-\infty}^{+\infty} \left| \frac{1}{\beta} e^{-\frac{\pi}{\beta^2} |x|^2} - \frac{1}{\alpha} e^{-\frac{\pi}{\alpha^2} |x|^2} \right| \, dx.
\]

Let \( x = \alpha y \), we get
\[
\int_0^1 |\psi_\beta(x) - \psi_\alpha(x)| \, dx \leq \int_{-\infty}^{+\infty} \left| \frac{1}{\beta/\alpha} e^{-\frac{\pi}{(\beta/\alpha)^2} |y|^2} - e^{-\pi |y|^2} \right| \, dy. \quad (3.3.12)
\]

Without loss of generality, assume \( \alpha = 1, \beta = 1 + \epsilon \), where \( 0 < \epsilon \leq 1 \), we estimate the right hand of (3.3.12)
\[
\int \left| e^{-\pi |x|^2} - \frac{1}{1 + \epsilon} e^{-\frac{\pi}{(1+\epsilon)^2} |x|^2} \right| \, dx \\
\leq \int \left| e^{-\pi |x|^2} - e^{-\frac{\pi}{(1+\epsilon)^2} |x|^2} \right| \, dx + \int (1 - \frac{1}{1 + \epsilon}) e^{-\frac{\pi}{(1+\epsilon)^2} |x|^2} \, dx \\
= \int \left| e^{-\pi |x|^2} - e^{-\frac{\pi}{(1+\epsilon)^2} |x|^2} \right| \, dx + \epsilon \\
= \int \left| 1 - e^{-\pi(1 - \frac{1}{(1+\epsilon)^2})x^2} \right| \cdot e^{-\frac{\pi}{(1+\epsilon)^2} x^2} \, dx + \epsilon.
\]

For \( \forall z \geq 0 \), we have
\[
1 - z \leq e^{-z} \leq 1 \Rightarrow 0 \leq 1 - e^{-z} \leq z,
\]
and
\[
\left| e^{-\pi(1 - \frac{1}{(1+\epsilon)^2})x^2} - 1 \right| \leq \pi (1 - \frac{1}{(1+\epsilon)^2}) x^2 \\
= \frac{\pi}{(1+\epsilon)^2} (2\epsilon + \epsilon^2) x^2 \leq 2\pi \epsilon x^2.
\]
Finally,

\[ \int_0^1 |\psi_\alpha(x) - \psi_\beta(x)| \, dx \leq 2\pi \varepsilon \int_{\mathbb{R}} x^2 e^{-\frac{\pi}{(1+\varepsilon)^2} x^2} \, dx + \varepsilon = \varepsilon + \varepsilon(1 + \varepsilon)^3 \leq 9\varepsilon. \]

Since \( \varepsilon = \frac{\beta}{\alpha} - 1 \), based on (3.3.12),

\[ \Delta(\psi_\alpha, \psi_\beta) = \frac{1}{2} \int_0^1 |\psi_\alpha(x) - \psi_\beta(x)| \, dx \leq \frac{9}{2} \left( \frac{\beta}{\alpha} - 1 \right). \]

We complete the proof of this lemma. \( \square \)

In order to obtain the discrete Gauss distribution on \( \mathbb{Z}_q \), we construct a discrete processing technique for continuous random variables. Let \( \mathbb{T} \) be any interval with length 1 on \( \mathbb{R} \), denoted as

\[ \mathbb{T} \equiv [0, 1) \pmod{1}. \]

If \( \varphi(x) \) is the density function of a continuous random variable \( \varphi \) on \( \mathbb{T} \), we define a discrete random variable \( \overline{\varphi} \) on \( \mathbb{Z}_q \) by

\[ \overline{\varphi} = [q \varphi], \quad (3.3.13) \]

that is, if \( \varphi \) takes a value \( x \in \mathbb{T} \), then \( \overline{\varphi} \) takes the value \( [qx] \pmod{q} \), where \( [x] \) is the closest integer to \( x \). When \( x \) runs over \( [0, 1) \), obviously \( [qx] \) runs over \( \mathbb{Z}_q \), so \( \overline{\varphi} \) defined in (3.3.13) is indeed a discrete random variable on \( \mathbb{Z}_q \). We call \( \overline{\varphi} \) the discretization of \( \varphi \).

**Lemma 3.3.6** If \( \varphi \) is a continuous random variable on \( \mathbb{T} \) with the density function \( \varphi(x) \), then \( \overline{\varphi} \) is a discrete random variable on \( \mathbb{Z}_q \), and its probability distribution \( \overline{\varphi}(k) \) is

\[ \Pr[\overline{\varphi} = k] = \overline{\varphi}(k) = \int_{(k-\frac{1}{2})/q}^{(k+\frac{1}{2})/q} \varphi(x) \, dx, \quad k \in \mathbb{Z}_q. \]

**Proof**

\[ \Pr[\overline{\varphi} = k] = \Pr[\lfloor q \varphi \rfloor = k] = \Pr\left\{ k - \frac{1}{2} \leq q \varphi < k + \frac{1}{2} \right\} \]

\[ = \Pr\left\{ \left( k - \frac{1}{2} \right) /q \leq \varphi < \left( k + \frac{1}{2} \right) /q \right\} = \int_{(k-\frac{1}{2})/q}^{(k+\frac{1}{2})/q} \varphi(x) \, dx. \]

\( \square \)
Definition 3.3.5 The discrete Gauss distribution $\overline{\psi}_\beta$ on $\mathbb{Z}_q$ is defined by

$$
\overline{\psi}_\beta(k) = \int_{(k-\frac{1}{2})/q}^{(k+\frac{1}{2})/q} \psi_\beta(x) \, dx,
$$

where $\psi_\beta(x)$ is the continuous Gauss distribution on $\mathbb{T}$ in (3.3.9) and $\beta$ is called the parameter of discrete Gauss distribution.

In the LWE problem, usually we suppose $\chi = \overline{\psi}_\beta$ is a discrete Gauss distribution. The main result in this chapter is the following theorem.

Theorem 3.3.1 Let $m = \text{Poly}(n)$, $q \leq 2^{\text{Poly}(n)}$, $\chi = \overline{\psi}_\alpha$ be the discrete Gauss distribution with parameter $\alpha$, where $0 < \alpha < 1$, and $\alpha q \geq 2\sqrt{n}$. Then the difficulty of solving the $\text{D-LWE}_{n,q,\chi,m}$ problem is at least as hard as that of $\text{GapSVP}_\gamma$ or $\text{SIVP}_\gamma$ problem on any $n$ dimensional full rank lattice $L$ based on quantum algorithm, where $\gamma = \tilde{O}(\frac{n}{\alpha})$.

The proof of Theorem 3.3.1 will be given in the next section. Here we only introduce the idea of this proof. The proof of Theorem 3.3.1 is mainly divided into the following two steps:

1. Using the quantum reduction algorithm to prove that the $\text{LWE}_{n,q,\chi,m}$ problem is at least as hard as difficult problems on any lattice such as the $\text{GapSVP}$ and $\text{SIVP}$ problems.

2. Prove the difficulty of the $\text{D-LWE}_{n,q,\chi,m}$ problem is not lower than that of the $\text{LWE}_{n,q,\chi,m}$ problem (see Theorem 3.4.1 in the next section). The original proof of the Theorem 3.4.1 is based on the modulus $q$ being a prime number, such as $q = 2$. Later it is generalized to the general case $q = 2^{\text{Poly}(n)}$ (see Regev (2009) and Peikert (2009)), and the proof of Theorem 3.3.1 is complete.

3.4 Proof of the Main Theorem

In this section, we mainly prove that the difficulty of solving $\text{D-LWE}$ problem is not lower than that of the hard problem on lattice, that is, if there is a quantum algorithm for solving the $\text{D-LWE}$ problem, then there exists a quantum algorithm to solve the hard problem on lattice. The whole proof could be divided into three parts. In order to better understand the three parts of proof, we first introduce the definition of the DGS problem.
Definition 3.4.1  DGS\(_\phi\): given an \(n\) dimensional lattice \(L\) with generated matrix \(B\), a real number \(r > \phi(B)\), where \(\phi\) is a real function of \(B\). The goal is to output a sample from the discrete Gauss distribution \(D_{L,r}\).

The DGS problem is also called the discrete Gauss sampling problem. We will see that the difficulty of the DGS problem is polynomial equivalent to that of the hard problem on lattice after this proof. Next we introduce the idea of proving that the D-LWE problem is at least as difficult as the hard problem on lattice. This proof could be divided into three parts, which are given in Sects. 3.4.1, 3.4.2 and 3.4.3. In Sect. 3.4.1, we prove that if there is a quantum algorithm to solve the LWE problem, then there is also a quantum algorithm to solve the DGS\(_{\sqrt{2n} \eta_\phi(L)/\alpha}\) problem. In Sect. 3.4.2, we give a reduction algorithm from the GIVP\(_{\sqrt{n} \phi}\) problem to the DGS\(_\phi\) problem, so that we have completed the proof that the LWE problem is not less difficult than the hard problem on lattice. In Sect. 3.4.3, we further prove that the D-LWE problem D-LWE\(_{n,q,\chi,m}\) can be reduced to the LWE\(_{n,q,\chi,m}\) problem and complete the proof of Theorem 3.3.1. The flowchart of the whole proof is shown in Fig. 3.1.

### 3.4.1 From LWE to DGS

In this subsection, we will solve the DGS\(_{\sqrt{2n} \eta_\phi(L)/\alpha}\) problem by the algorithm of LWE\(_{n,q,\psi_m}\) problem. The main conclusion is the following Lemma 3.4.1, and its proof depends on Lemmas 3.4.2 and 3.4.3. We give these three lemmas first.
Lemma 3.4.1 Let \( m = \text{Poly}(n), \epsilon = \epsilon(n) \) be a negligible function of \( n \), \( q = q(n) \) be a positive integer, \( \alpha = \alpha(n) \in (0, 1), \alpha q \geq 2\sqrt{n}, \chi = \psi_\alpha \). Assume that we have an algorithm \( W \) that solves the \( \text{LWE}_{n,q,\psi_\alpha,m} \) problem given a polynomial number of samples, then there exists an efficient quantum algorithm for the \( \text{DGS}_{\sqrt{2n\eta_\epsilon(L)}/\alpha} \) problem.

Lemma 3.4.2 For any \( n \) dimensional lattice \( L \) and a real number \( r > 2^{2^nn^{\lambda_n}}(L) \), there exists an efficient algorithm that outputs a sample from a distribution that is within statistical distance \( 2^{-\Omega(n)} \) of the discrete Gauss distribution \( D_{L,r} \), where \( \Omega(n) \) is a polynomial function or exponential function of \( n \).

Lemma 3.4.3 Let \( m = \text{Poly}(n), \epsilon = \epsilon(n) \) be a negligible function of \( n \), \( q = q(n) \geq 2 \) be a positive integer, \( \alpha = \alpha(n) \in (0, 1) \). Assume that we have an algorithm \( W \) that solves the \( \text{LWE}_{n,q,\psi_\alpha,m} \) problem given a polynomial number of samples, then there exists a constant \( c > 0 \) and an efficient quantum algorithm that, given any \( n \) dimensional lattice \( L \), a real number \( r > \sqrt{2q\eta_\epsilon(L)} \) and \( n^{c} \) samples from \( D_{L,r} \), outputs a sample from \( D_{L,r^{n}q\eta_\epsilon(L)}/(\epsilon\alpha^{q}) \).

Proof of Lemma 3.4.1: Given an \( n \) dimensional lattice \( L \) and a real number \( r > \sqrt{2n\eta_\epsilon(L)}/\alpha \), our goal is to output a sample from the discrete Gauss distribution \( D_{L,r} \). The idea of this proof is to use iteration steps. Let \( r_{i} = r(\alpha q/\sqrt{n})^{i}, \ i = 1, 2, \ldots, 3n \).

Based on Lemma 1.3.6 in Chap. 1,

\[
r_{3n} > 2^{3n}r > 2^{3n}\sqrt{2n\eta_\epsilon(L)}/\alpha \geq 2^{3n}\sqrt{2n}\frac{\ln 1/\epsilon \lambda_n(L)}{\pi} > 2^{2n}\lambda_n(L).
\]

By Lemma 3.4.2, we can produce samples from the discrete Gauss distribution \( D_{L,r_{3n}} \). Suppose \( c \) is the constant from Lemma 3.4.3, we output \( n^{c} \) samples from \( D_{L,r_{3n}} \). According to Lemma 3.4.3, we can get samples from the distribution \( D_{L,r_{3n}\sqrt{n}/(\epsilon\alpha^{q})} \), i.e. \( D_{L,r_{3n-1}} \). Repeat this process, since

\[
r_{1} = r\alpha q/\sqrt{n} > \sqrt{2n\eta_\epsilon(L)}/\alpha \cdot \alpha q/\sqrt{n} = \sqrt{2q\eta_\epsilon(L)},
\]

which satisfies the condition of Lemma 3.4.3, finally we can output a sample from \( D_{L,r_{1}\sqrt{n}/(\epsilon\alpha^{q})} = D_{L,r} \). The lemma holds.

Proof of Lemma 3.4.2: By the LLL algorithm (Lenstra et al. (1982)), we can choose the generated matrix \( B = [b_{1}, b_{2}, \ldots, b_{n}] \) of \( L \) satisfying \( b_{i} \leq 2^{\lambda_n(L)}, 1 \leq i \leq n \). Suppose \( F(B) \) is the basic neighborhood of lattice \( L \). The algorithm in Lemma 3.4.2 can be achieved by the following steps. First we generate a sample \( y \) from the discrete Gauss distribution \( D_{r} \), where

\[
D_{r}(x) = \frac{\rho_{r}(x)}{r^{n}}, \forall x \in \mathbb{R}^{n}.
\]
3.4 Proof of the Main Theorem

We get \( y' = y \mod L \in F(B) \), and \( x = y - y' \in L \). Denote the distribution of \( x \) as \( \xi \), next we prove the statistical distance between \( \xi \) and \( D_{L,r} \) is exponentially small. Note that

\[
|y'| \leq \text{diam}(F(B)) \leq \sum_{i=1}^{n} |b_i| \leq 2^{n} \lambda_n(L),
\]

where

\[
\text{diam}(F(B)) = \max \{|u - v| \mid u, v \in F(B)\}.
\]

Based on Lemma 1.3.4 in Chap. 1,

\[
\rho(L \setminus \sqrt{n} r N) < (r \sqrt{2 \pi e} e^{-\pi r^2})^n \rho(L),
\]

here \( N \) is the unit ball. This means \( \rho(L \setminus \sqrt{n} r N) \) is exponentially small, so we can always assume \( x \leq \sqrt{n} r \). By Lemma 3.3.4, let \( t = \sqrt{n} r \), \( l = n 2^{n} \lambda_n(L) \), by some simple calculations we get

\[
\Pr[\xi = x] = \int_{x + F(B)} D_r(y) dy \geq \int_{x + F(B)} (1 - 2^{-\Omega(n)}) D_r(x) dy
\]

\[
= (1 - 2^{-\Omega(n)}) D_r(x) \det(L).
\]

On the other hand, from Lemma 1.3.2 in Chap. 1,

\[
\Pr[D_{L,r} = x] = \frac{\rho_r(x)}{\rho_r(L)} = \frac{\rho_r(x)}{\det(L^*) r^n \rho_{1/r}(L^*)} \leq \frac{\rho_r(x)}{\det(L^*) r^n} = D_r(x) \det(L).
\]

So we have

\[
\Pr[\xi = x] \geq (1 - 2^{-\Omega(n)}) \Pr[D_{L,r} = x].
\]

Summing \( x \in L \) on both sides, we get the statistical distance between \( \xi \) and \( D_{L,r} \) is exponentially small. The lemma holds. \( \square \)

**Definition 3.4.2** (1) \( \text{CVP}_{L,d}: \) given an \( n \) dimensional lattice \( L \), a target vector \( t \in \mathbb{R}^n \), a real number \( d \), \( \text{dist}(t, L) \leq d \), find \( u \in L \) such that

\[
|u - t| = \min_{x \in L, |x - t| \leq d} |x - t|.
\]

(2) \( \text{CVP}_{q}^{(l)}: \) given an \( n \) dimensional lattice \( L \) with generated matrix \( B \), a target vector \( t \in \mathbb{R}^n \), a real number \( d \), \( \text{dist}(t, L) \leq d \), denote \( K_L(t) = \{ u \in L \mid |u - t| = \min_{x \in L} |x - t| \} \), i.e. \( K_L(t) \) is the closest vector to \( t \) in the lattice \( L \), output \( B^{-1} K_L(t) \mod q \in \mathbb{Z}^n_q \).
The CVP problem is also called the closest vector problem. In order to prove Lemma 3.4.3, we need the following two lemmas, Lemmas 3.4.4 and 3.4.14. In Lemma 3.4.4, we use the samples of \( D_{L,r} \) to solve the CVP \( L^{*},aq/(\sqrt{2}r) \) problem, and Lemma 3.4.14 shows that we can generate a sample of \( D_{L,r,\sqrt{n}/aq} \) from the algorithm of solving the CVP \( L^{*},aq/(\sqrt{2}r) \) problem so that we complete the proof of Lemma 3.4.3. The following content is divided into two parts. In the first part, we use Lemmas 3.4.5 to 3.4.11 to prove Lemma 3.4.4, which is to solve the CVP \( L^{*},aq/(\sqrt{2}r) \) problem based on the samples of \( D_{L,r} \). In the second part, we prove Lemma 3.4.14 according to Lemmas 3.4.12 and 3.4.13, and achieve the transition from solving CVP \( L^{*},aq/(\sqrt{2}r) \) to \( D_{L,r,\sqrt{n}/aq} \).

**Lemma 3.4.4** Let \( m = \text{Poly}(n) \), \( \varepsilon = \varepsilon(n) \) be a negligible function of \( n \), \( q = q(n) \geq 2 \) be a positive integer, \( \alpha = \alpha(n) \in (0, 1) \). Assume that we have an algorithm \( W \) that solves \( \text{LWE}_{n,q,\psi_{\alpha},m} \) given a polynomial number of samples, then there exists a constant \( c > 0 \) and an efficient algorithm that, given any \( n \) dimensional lattice \( L \), a real number \( r > \sqrt{2}q \eta_{\varepsilon}(L) \), and \( n^{c} \) samples from \( D_{L,r} \), solves the CVP \( L^{*},aq/(\sqrt{2}r) \) problem.

**Proof** This lemma is proved directly by the following Lemmas 3.4.5 to 3.4.11. □

Lemma 3.4.5 shows the relationship of difficulty between the CVP and CVP\((q)\) problems.

**Lemma 3.4.5** Given an \( n \) dimensional lattice \( L \), a real number \( d < \lambda_{1}(L)/2 \), \( q \geq 2 \) is a positive integer. There exists an efficient algorithm to solve the CVP\((q)_{L,d}\) problem based on the algorithm for CVP\((q)\).

**Proof** Let \( x \in \mathbb{R}^{n} \) satisfying \( \text{dist}(x, L) \leq d \) be the target vector, define vectors \( \{x_{n}\} \) and \( \{a_{n}\} \) as follows: \( x_{1} = x \),

\[
a_{i} = B^{-1}K_{L}(x_{i}) \in \mathbb{Z}^{n} , \quad i \geq 1,
\]

which is the coefficient vector of the closest vector to \( x_{i} \) in lattice \( L \),

\[
x_{i+1} = (x_{i} - B(a_{i} \mod q))/q , \quad i \geq 1,
\]

it is easy to prove

\[
a_{i+1} = (a_{i} - (a_{i} \mod q))/q ,
\]

and

\[
|x_{i+1} - Ba_{i+1}| \leq \frac{d}{q^{i}}.
\]

That is, the distance from \( x_{n+1} \) to lattice \( L \) is no more than \( \frac{d}{q^{n}} \). Note that \( \frac{d}{q^{n}} \) could be sufficiently small if \( n \) becomes lager enough. Based on the nearest plane algorithm
by Babai (1985), we can find \( y \in L \) such that \( y \) is the closest vector to \( x_{n+1} \) in lattice \( L \). Let \( y = Ba \), then \( a_{n+1} = a \), combine with

\[
a_{i+1} = (a_i - (a_i \mod q))/q,
\]

we get \( a_n, a_{n-1}, \ldots, a_1 \), and complete the process of solving the CVP\(_{L,d}\) problem. This lemma holds.

We introduce the definition of the LWE distribution \( A_{s,\chi} \) in Definition 3.3.2, where \( \chi \) is a distribution on \( \mathbb{Z}_q \). If the value space of \( \chi \) is changed to \( T = [0, 1) \), we can give another definition of LWE distribution.

**Definition 3.4.3** Let \( s \in \mathbb{Z}_q^n \), \( e \) be a random variable on \( T \) with density function \( \phi \). The LWE distribution \( A_{s,\phi} = (a, b) \in \mathbb{Z}_q^n \times T \) generated by \( s \) and \( \phi \) satisfies:

1. \( a \in \mathbb{Z}_q^n \) is uniformly distributed.
2. \( b = a \cdot s/q + e \mod 1 \).

The LWE distribution we discuss later in this section is always \( A_{s,\phi} \).

**Lemma 3.4.6** Let \( q = q(n) \geq 1 \) be a positive integer, given \( s' \in \mathbb{Z}_q^n \) and samples from \( A_{s,\psi_\alpha} \) for some unknown \( s \in \mathbb{Z}_q^n \), \( \alpha < 1 \). There exists an efficient algorithm that determines whether \( s' = s \) with probability exponentially close to 1.

**Proof** Let \((a, x)\) be a sample from the LWE distribution \( A_{s,\psi_\alpha} \), \( T = [0, 1) \), \( \xi \) be a random variable on \( T \) with density function \( p(y) \) such that

\[
\xi = x - a \cdot s'/q = e + a \cdot (s - s')/q. \tag{3.4.1}
\]

The steps of the algorithm are as follows. Generate \( n \) samples \( y_1, y_2, \ldots, y_n \) of \( \xi \) and compute

\[
z = \frac{1}{n} \sum_{i=1}^{n} \cos(2\pi y_i).
\]

If \( z > 0.02 \), then we confirm \( s = s' \), otherwise, we decide \( s \neq s' \). Next we prove the correctness of this algorithm.

If \( s = s' \), by (3.4.1) we get \( \xi = e \) with the distribution \( \psi_\alpha \). On the other hand, if \( s \neq s' \), then there is \( 1 \leq j \leq n \), such that \( s_j \neq s'_j \), where \( s_j \) and \( s'_j \) are the \( j \)th coordinates of \( s \) and \( s' \), respectively. Let \( g = \gcd(q, s_j - s'_j) \), \( k = q/\gcd(q, s_j - s'_j) \), \( a_j \) be the \( j \)th coordinate of \( a \), it is not hard to see the distribution of \( a_j(s_j - s'_j) \mod q \) has period \( g \), i.e. the distribution of \( a_j(s_j - s'_j)/q \mod 1 \) has period \( g/q = 1/k \), \( k \geq 2 \). Since \( \xi \) is regarded as the sum of \( a_j(s_j - s'_j)/q \mod 1 \) and an independent random variable, therefore, the distribution of \( \xi \) also has period \( 1/k \). Assume \( \bar{z} \) is the expectation of \( \cos(2\pi \xi) \),
\[
\tilde{z} = E[\cos(2\pi \xi)] = \int_0^1 \cos(2\pi y) p(y) dy = \Re \int_0^1 e^{2\pi i y} p(y) dy.
\]

When \( s = s' \), the distribution of \( \xi \) is \( \psi_\alpha \), the right hand of the above formula could be computed as \( \tilde{z} = e^{-\pi \alpha^2} \). When \( s \neq s' \), the distribution of \( \xi \) is periodic with period \( 1/k \), note that the integral of the periodic function \( e^{2\pi i y} p(y) \) with period 1 is fixed in any interval of length 1, then

\[
\int_0^1 e^{2\pi i y} p(y) dy = \int_{1/k}^{1} e^{2\pi i y} p(y) dy
\]

\[
= \int_0^1 e^{2\pi i (y + \frac{1}{k})} p(y) dy
\]

\[
= e^{2\pi i \frac{1}{k}} \int_0^1 e^{2\pi i y} p(y) dy.
\]

From \( k \geq 2 \) we know \( \tilde{z} = 0 \), by the Chebyshev inequality,

\[
Pr\{|z - \tilde{z}| \leq 0.01\} \geq 1 - \frac{\text{Var}[\cos(2\pi \xi)]}{0.01^2 n}.
\]

The probability of \( |z - \tilde{z}| \leq 0.01 \) is exponentially close to 1 when \( n \) is large enough. Thus, we confirm \( s \neq s' \) with probability exponentially close to 1 if \( z \leq 0.02 \). We complete the proof. \( \square \)

Based on Lemma 3.4.6 and the algorithm for LWE\(_{n,q,\psi_\alpha,m}\), for any \( \beta \leq \alpha \) and samples from \( A_{s,\psi_\beta} \), the following Lemma 3.4.7 gives an algorithm to solve \( s \) with probability close to 1.

**Lemma 3.4.7** Let \( q = q(n) \geq 2 \) be a positive integer, \( \alpha = \alpha(n) \in (0, 1) \). Assume that we have an algorithm \( W \) that solves LWE\(_{n,q,\psi_\alpha,m}\) with a polynomial number of samples, then there exists an efficient algorithm \( W' \) to solve \( s \) with probability exponentially close to 1 for some samples from \( A_{s,\psi_\beta} \), where \( \beta \leq \alpha \) and \( \beta \) is unknown.

**Proof** Assume we need \( n^c \) samples in the algorithm \( W \), \( c > 0 \) is a constant. Let the set \( Z \) be

\[
Z = \{ \gamma \mid \gamma = \delta n^{-2c} \alpha^2 \in [0, \alpha^2], \ \delta \in \mathbb{Z} \}.
\]

The steps of algorithm \( W' \) are as follows. For each \( \gamma \in Z \), we repeat the following process \( n \) times. Each time we get \( n^c \) samples from \( A_{s,\psi_\beta} \) and add samples from
ψ√γ to the second component of each sample from A_{s,ψγ}, so we obtain \( n^c \) samples from \( A_{s,ψ\sqrt{\Gamma}} \). We solve \( s' \) by algorithm \( W \) and determine whether \( s' = s \). If \( s' = s \), output \( s' \) and we complete the algorithm. Next we prove that the above algorithm could achieve the goal of solving \( s \) with probability exponentially close to 1. Assume
\[
\Gamma = \min\{\gamma \in \mathbb{Z}, \gamma \geq \alpha^2 - \beta^2\}.
\]
From the definition of the set \( Z \)
\[
\Gamma \leq \alpha^2 - \beta^2 + n^{-2c}\alpha^2.
\]
Let \( \alpha' = \sqrt{\beta^2 + \Gamma} \), we have
\[
\alpha \leq \alpha' \leq \sqrt{\alpha^2 + n^{-2c}\alpha^2} \leq (1 + n^{-2c})\alpha.
\]
Based on lemma 3.3.5,
\[
\Delta(\psi_\alpha, \psi_{\alpha'}) \leq \frac{9}{2} \left( \frac{\alpha'}{\alpha} - 1 \right) \leq \frac{9}{2} n^{-2c}.
\]
Therefore, the statistical distance between the \( n^c \) samples from \( \psi_\alpha \) and \( n^c \) samples from \( \psi_{\alpha'} \) is no more than \( 9n^{-c} \), which means the probability that the algorithm \( W \) solves \( s \) successfully is at least \( 1 - 9n^{-c} \geq \frac{1}{2} \). It follows that the probability of solving \( s \) unsuccessfully \( n \) times is no more than \( 2^{-n} \). The lemma holds.

To prove our main result, we need two properties about the Gauss function and statistical distance.

**Lemma 3.4.8** For any \( n \) dimensional lattice \( L \), \( c \in \mathbb{R}^n \), \( \varepsilon > 0 \), \( r \geq \eta_c(L) \), we have
\[
\rho_r(L + c) \in r^n \det(L^*)(1 \pm \varepsilon).
\]

**Proof** Based on Lemma 1.3.2 in Chap. 1,
\[
\rho_r(L + c) = \sum_{x \in L} \rho_{r-c}(x) = \det(L^*) \sum_{y \in L^*} \hat{\rho}_{r-c}(y)
\]
\[
= r^n \det(L^*) \sum_{y \in L^*} e^{2\pi i c \cdot y} \rho_{1/r}(y)
\]
\[
= r^n \det(L^*) (1 + \sum_{y \in L^* \setminus \{0\}} e^{2\pi i c \cdot y} \rho_{1/r}(y)).
\]
From \( r \geq \eta_c(L) \), it follows that \( \rho_{1/r}(L^* \setminus \{0\}) \leq \varepsilon \), and
\[
\left| \sum_{y \in L^* \setminus \{0\}} e^{2\pi i c \cdot y} \rho_{1/r}(y) \right| \leq \sum_{y \in L^* \setminus \{0\}} \rho_{1/r}(y) \leq \varepsilon.
\]

We get
\[
\rho_r(L + c) = r^n \det(L^*) \left( 1 + \sum_{y \in L^* \setminus \{0\}} e^{2\pi i c \cdot y} \rho_{1/r}(y) \right) \in r^n \det(L^*)(1 \pm \varepsilon).
\]

The proof is complete. \qed

**Lemma 3.4.9** For any \(n\) dimensional lattice \(L, u \in \mathbb{R}^n, \varepsilon < \frac{1}{2}, r, s\) are two positive real numbers, \(t = \sqrt{r^2 + s^2}\), assume \(rs/t = 1/\sqrt{1/r^2 + 1/s^2} \geq \eta_r(L)\), let \(\xi\) be the sum of a discrete Gauss distribution \(D_{L + u, r}\) and a noise distribution \(D_s\), then
\[
\Delta(\xi, D_t) \leq 2\varepsilon. \tag{3.4.3}
\]

**Proof** Let the density function of \(\xi\) be \(Y(x)\), then
\[
Y(x) = \frac{1}{s^n \rho_r(L + u)} \sum_{y \in L + u} \rho_r(y) \rho_s(x - y)
\]
\[
= \frac{1}{s^n \rho_r(L + u)} \sum_{y \in L + u} \exp \left( -\pi \left( \frac{|y|^2}{r} + \frac{|x - y|^2}{s} \right) \right)
\]
\[
= \frac{1}{s^n \rho_r(L + u)} \sum_{y \in L + u} \exp \left( -\pi \left( \frac{r^2 + s^2}{r^2 s^2} \left| y - \frac{r^2}{r^2 + s^2} x \right|^2 \right) + \frac{1}{r^2 + s^2} |x|^2 \right)
\]
\[
= \exp \left( -\frac{\pi}{r^2 + s^2} |x|^2 \right) \frac{1}{s^n \rho_r(L + u)} \sum_{y \in L + u} \exp \left( -\pi \left( \frac{r^2 + s^2}{r^2 s^2} \left| y - \frac{r^2}{r^2 + s^2} x \right|^2 \right) + \frac{1}{r^2 + s^2} |x|^2 \right)
\]
\[
= \frac{\hat{\rho}_r(x)}{s^n} \frac{\rho_{rs/t}(r/t)^2 x - u(L)}{\hat{\rho}_{r, -u}(L)}
\]
\[
= \frac{\rho_r(x)}{s^n} \frac{\hat{\rho}_{rs/(t, (r/t)^2)}(r/t)^2 x - u(L^*)}{\hat{\rho}_{r, -u}(L^*)}
\]
\[
= \frac{\rho_r(x)}{t^n} \frac{(r/s)^n \hat{\rho}_{rs/(t, (r/t)^2)} x - u(L^*)}{(1/r)^n \hat{\rho}_{r, -u}(L^*)}. \tag{3.4.4}
\]

Based on the Fourier transform property of Gauss function in Lemma 1.2.1 in Chap. 1, we get
\[
\hat{\rho}_{rs/(t, (r/t)^2) x - u}(w) = \exp(-2\pi i ((r/t)^2 x - u) \cdot w)(rs/t)^n \rho_{t/rs}(w),
\]
and
\[ \hat{\rho}_{r-u}(w) = \exp(2\pi i u \cdot w)r^n \rho_{1/r}(w). \]

Since \( r \geq \frac{rs}{t} \geq \eta_t(L) \),
\[ |1 - (t/rs)^n \hat{\rho}_{rs/(r/t)^2 x-u}(L^*)| \leq \rho_{t/rs}(L^*\setminus\{0\}) \leq \varepsilon, \]
\[ |1 - (1/r)^n \hat{\rho}_{r-u}(L^*)| \leq \rho_{1/r}(L^*\setminus\{0\}) \leq \varepsilon. \]

It follows that
\[ 1 - 2\varepsilon \leq \frac{1 - \varepsilon}{1 + \varepsilon} \leq \frac{(t/rs)^n \hat{\rho}_{rs/(r/t)^2 x-u}(L^*)}{(1/r)^n \hat{\rho}_{r-u}(L^*)} \leq \frac{1 + \varepsilon}{1 - \varepsilon} \leq 1 + 4\varepsilon. \]

By (3.4.4),
\[ |Y(x) - \frac{\rho_t(x)}{t^n}| \leq 4\varepsilon \frac{\rho_t(x)}{t^n}. \]

Integrate for \( x \in \mathbb{R}^n \),
\[ \Delta(\xi, D_t) = \frac{1}{2} \int_{\mathbb{R}^n} |Y(x) - \frac{\rho_t(x)}{t^n}| dx \leq 2\varepsilon. \]

We complete the proof. \( \square \)

**Lemma 3.4.10** For any \( n \) dimensional lattice \( L \), vectors \( z, u \in \mathbb{R}^n \), real numbers \( r, \alpha > 0, \varepsilon < \frac{1}{2}, \eta_t(L) \leq 1/\sqrt{1/r^2 + (|z|/\alpha)^2} \), let \( v \) be a random variable of the discrete Gauss distribution \( D_{L+u,r} \), \( e \) be a random variable of Gauss distribution with mean 0 and standard deviation \( \alpha/\sqrt{2\pi} \), \( \xi \) be a random variable of Gauss distribution with mean 0 and standard deviation \( \sqrt{(r|z|)^2 + \alpha^2}/\sqrt{2\pi} \), then
\[ \Delta(z \cdot v + e, \xi) \leq 2\varepsilon. \] (3.4.5)

In particular,
\[ \Delta(z \cdot v + e \mod 1, \psi \sqrt{(r|z|)^2 + \alpha^2}) \leq 2\varepsilon. \] (3.4.6)

**Proof** Let the random variable \( h \) has distribution \( D_{\alpha/|z|} \), then the standard deviation of \( h \) is \( \alpha/(|z|\sqrt{2\pi}) \), and the standard deviation of \( z \cdot h \) is \( |z| \cdot \alpha/(|z|\sqrt{2\pi}) = \alpha/\sqrt{2\pi} \) which is the same as that of \( e \). Since both of them have Gauss distributions, we get the distributions of \( z \cdot h \) and \( e \) are the same, i.e. \( z \cdot v + e \) and \( z \cdot (v + h) \) have the same distribution. Based on Lemma 3.4.9, let \( s = \alpha/|z| \), it follows that the statistical distance between \( v + h \) and \( D_{\sqrt{r^2 + (\alpha/|z|)^2}} \) is no more than \( 2\varepsilon \),
\[ \Delta(v + h, D_{\sqrt{r^2 + (\alpha/|z|)^2}}) \leq 2\varepsilon. \]
By the property of statistical distance,
\[ \Delta(z \cdot (v + h), z \cdot D^{\sqrt{r^2 + (\alpha/|z|)^2}}) \leq 2\varepsilon. \]

Here the standard deviation of \( z \cdot D^{\sqrt{r^2 + (\alpha/|z|)^2}} \) is
\[ |z| \cdot \sqrt{r^2 + (\alpha/|z|)^2} / \sqrt{2\pi} = \sqrt{(r|z|)^2 + \alpha^2 / \sqrt{2\pi}}, \]
which is the same as that of \( \xi \). Note that both of the two random variables have Gauss distributions; therefore, \( z \cdot D^{\sqrt{r^2 + (\alpha/|z|)^2}} \) and \( \xi \) have the same distribution, i.e.
\[ \Delta(z \cdot v + e, \xi) \leq 2\varepsilon, \]
mod 1 for both of the two random variables,
\[ \Delta(z \cdot v + e \mod 1, \psi^{\sqrt{(r|z|)^2 + \alpha^2}}) \leq 2\varepsilon. \]

The lemma holds. \( \square \)

**Lemma 3.4.11** Let \( \varepsilon = \varepsilon(n) \) be a negligible function of \( n \), \( q = q(n) \geq 2 \) be a positive integer, \( \alpha = \alpha(n) \in (0, 1) \). Assume we have an algorithm \( W \) to solve \( s \) given a polynomial number of samples from \( A_{s,psi} \) for any \( \beta \leq \alpha \) (\( \beta \) is unknown), then there exists an efficient algorithm that given an \( n \) dimensional lattice \( L \), a real number \( r > \sqrt{2}q\eta_e(L) \) and a polynomial number of samples from \( D_{L,r} \), to solve the CVP\((q)_{L^*,\alpha q/(\sqrt{2}r)} \) problem.

**Proof** For a given \( x \in \mathbb{R}^n \), \( \text{dist}(x, L^*) \leq \alpha q / (\sqrt{2}r) \), denote the generated matrix of \( L \) is \( B \), and the generated matrix of \( L^* \) is \((B^T)^{-1} \), our goal is to solve \( s = B^{-1}v \mod q \). The idea of algorithm \( W' \) is to generate a polynomial number of samples from \( A_{s,psi} \), and solve \( s \) according to the algorithm \( W \).

The steps of algorithm \( W' \) are as follows: let \( v \in L \) be a sample from the discrete Gauss distribution \( D_{L,r} \), \( a = B^{-1}v \mod q \), \( e \) be random variable of Gauss distribution with mean 0 and standard deviation \( \alpha / (2\sqrt{\pi}) \), then there is \( \beta \leq \alpha \) such that the statistical distance between \((a, x \cdot v/q + e \mod 1)\) and \( A_{s,psi} \) is negligible. Next we prove the correctness of this algorithm.

Firstly, note that the distribution of \( a \) is almost uniform, i.e. the statistical distance between \( a \) and the uniform distribution is negligible. This is because for any \( a_0 \in \mathbb{Z}_q^n \), we have
\[ \Pr[a = a_0] = \rho_{r}(qL + Ba_0) = \rho_{r/q}(L + Ba_0/q). \]

Since \( q\eta_e(L) < r \), based on Lemma 3.4.8,
\[ \Pr[a = a_0] = \rho_{r/q}(L + Ba_0/q) \in (r/q)^n \det(L^*)(1 \pm \varepsilon), \forall a_0 \in \mathbb{Z}_q^n. \]
This implies $a$ is almost uniformly distributed.

Secondly, we consider the distribution of $x \cdot v/q + e \mod 1$. Let $x' = x - K_{L^*}(x)$, from $\text{dist}(x, L^*) \leq \alpha q/\sqrt{2r}$ we get $|x'| \leq \alpha q/\sqrt{2r}$ and

$$x \cdot v/q + e \mod 1 = (x'/q) \cdot v + e + K_{L^*}(x) \cdot v/q \mod 1. \quad (3.4.7)$$

We compute the distributions of $K_{L^*}(x) \cdot v/q \mod 1$ and $(x'/q) \cdot v + e$, respectively. It is easy to see

$$K_{L^*}(x) \cdot v = (B^T K_{L^*}(x)) \cdot (B^{-1} v),$$

therefore,

$$K_{L^*}(x) \cdot v \mod q = (B^T K_{L^*}(x)) \cdot (B^{-1} v) \mod q = s \cdot a \mod q.$$

This means $K_{L^*}(x) \cdot v/q \mod 1$ and $s \cdot a/q \mod 1$ have the same distribution. In order to get the distribution of $(x'/q) \cdot v + e$, note that $v$ has discrete Gauss distribution $D_{qL^*} + Ba \cdot r$, and $e$ has Gauss distribution with mean 0 and standard deviation $\alpha/(2\sqrt{\pi})$, let $\beta = \sqrt{(r|x'|^2/q^2) + \alpha^2/2} \leq \alpha$,

$$1/\sqrt{1/r^2 + (\sqrt{2}|x'|/\alpha q)^2} \geq r/\sqrt{2} > q \eta_L(L) = \eta_L(q L)$$

satisfies the condition of Lemma 3.4.10. By Lemma 3.4.10, $(x'/q) \cdot v + e$ almost has the distribution $\psi_\beta$ and the statistical distance of them is negligible. From (3.4.7), $x \cdot v/q + e \mod 1$ and $\psi_\beta + s \cdot a/q \mod 1$ have the same distribution. Above all, we get the statistical distance between $(a, x \cdot v/q + e \mod 1)$ and $A_s \psi_\beta$ is negligible so that the algorithm $W'$ is correct. We complete the proof. \qed

Combining the above Lemmas 3.4.5, 3.4.7 and 3.4.11, we obtain the conclusion of Lemma 3.4.4 immediately, which shows that we can solve the CVP $L^*, \alpha q/(\sqrt{2r})$ problem by the samples of $D_{qL^*}$. In order to prove Lemma 3.4.3 completely, we introduce the technique of quantum computation to prove there is an efficient quantum algorithm to generate a sample from $D_{qL^*\sqrt{q}/\alpha q}$ based on the algorithm for the CVP $L^*, \alpha q/(\sqrt{2r})$ problem.

**Definition 3.4.4** For a real number $a \in \mathbb{R}$ and a vector $x \in \mathbb{R}^n$, we define the Dirac notation $a|x\rangle = ax$. Let $A$ be a finite or countable set in $\mathbb{R}^n$, $f$ be a function from $\mathbb{R}^n$ to $\mathbb{R}$, a quantum state is defined by

$$\sum_{x \in A} f(x)|x\rangle = \sum_{x \in A} f(x)x, \quad (3.4.8)$$

if $\sum_{x \in A} f(x)x$ converges.
The knowledge about Dirac notation and quantum state is an important part of quantum physics. Since it involves too much content beyond the scope of this book, we will not introduce it in detail. We only provide the Lemmas 3.4.12, 3.4.13 and 3.4.14 here. The readers could refer to Nielsen and Chuang (2000), Shor (1997) for details. The following Lemma 3.4.12 gives the discrete Gauss quantum state on lattice, where the lattice $L$ satisfies $L \subset \mathbb{Z}^n$.

**Lemma 3.4.12** Given an $n$ dimensional lattice $L \subset \mathbb{Z}^n$, $r > 2^{2n} \lambda_n(L)$, there exists an efficient quantum algorithm to output a state within negligible $l_2$ distance from the following state

$$\sum_{x \in L} \sqrt{\rho_r(x)}|x\rangle = \sum_{x \in L} \rho_{\sqrt{\Sigma}}(x)|x\rangle.$$  

(3.4.9)

Let $L$ be an $n$ dimensional lattice, $R$ be a positive number, $L/R = \{x/R \mid x \in L\}$ be a lattice obtained by scaling down $L$ by a factor of $R$. The following lemma 3.4.13 claims that the quantum state on lattice is on points of norm at most $\sqrt{n}$.

**Lemma 3.4.13** Let $R$ be a positive integer, $L$ be an $n$ dimensional lattice such that $\lambda_1(L) > 2\sqrt{n}$, $F$ be the basic neighborhood of $L$. $v_1$ and $v_2$ are defined by

$$v_1 = \sum_{x \in L/R, |x| < \sqrt{n}} \rho(x)|x \mod L\rangle.$$  

(3.4.10)

and

$$v_2 = \sum_{x \in L/R} \rho(x)|x \mod L\rangle = \sum_{L/R \cap F} \sum_{y \in L} \rho(x - y)|x\rangle.$$  

(3.4.11)

Then the $l_2$ distance between $\frac{v_1}{|v_1|}$ and $\frac{v_2}{|v_2|}$ is negligible.

The following Lemma 3.4.14 gives an algorithm to generate a sample from $D_{L, \sqrt{n}/(\sqrt{2}d)}$ based on the algorithm for the CVP $L^*, d$ problem.

**Lemma 3.4.14** Given an $n$ dimensional lattice $L$, a real number $d < \lambda_1(L^*)/2$, if there exists an algorithm to solve the CVP $L^*, d$ problem, then there is an efficient quantum algorithm to generate a sample from the discrete Gauss distribution $D_{L, \sqrt{n}/(\sqrt{2}d)}$.

According to Lemma 1.3.6 in Chap. 1, when $r > \sqrt{2}q\eta_\epsilon(L)$, we have

$$\frac{\alpha q}{\sqrt{2}r} \leq \frac{\alpha}{2\eta_\epsilon(L)} \leq \frac{\alpha}{2} \sqrt{\frac{\pi}{\ln(1/\epsilon)}\lambda_1(L^*)} < \frac{\lambda_1(L^*)}{2},$$
replace $d$ in Lemma 3.4.14 with $aq/\sqrt{2}r$, then there exists a quantum algorithm to generate a sample from the discrete Gauss distribution $D_{L,r\sqrt{\pi}/aq}$ given the algorithm for the CVP$_{L^*,aq/\sqrt{2}r}$ problem.

Combine Lemma 3.4.4 with Lemma 3.4.14, for $r > \sqrt{2}q\eta_e(L)$, we have proved that one can solve the CVP$_{L^*,aq/\sqrt{2}r}$ problem given the algorithm for the LWE$_{n,q,\psi_\alpha,m}$ problem and a polynomial number of samples from $D_{L,r}$, and further to generate a sample from $D_{L,r,\sqrt{\pi}/aq}$, which is the whole proof of Lemma 3.4.3. So far, we get the main Lemma 3.4.1 in this subsection and finish the first part of proof for Theorem 3.3.1, i.e. from the algorithm for LWE$_{n,q,\psi_\alpha,m}$ problem to solve the DGS$_{\sqrt{2}n\eta_e(L)/\alpha}$ problem.

### 3.4.2 From DGS to Hard Problems on Lattice

In this subsection, we are to prove that if there is an algorithm to solve the DGS problem, then there exists a probabilistic polynomial algorithm to solve the hard problems on lattice. Take the GIVP problem as an example, that is, find a set $S = \{s_i\} \subset L$ of $n$ linearly independent vectors in $L$, such that

$$|S| = \max |s_i| \leq \gamma(n)\phi(B),$$

where $\gamma(n) \geq 1$ is a function of $n$, $B$ is the generated matrix of $L$, $\phi(B)$ is a real function of $B$. Specially, if $\phi = \lambda_n$, then the GIVP problem becomes the SIVP problem. In order to complete the proof of reduction algorithm from the hard problems on lattice to the DGS problem, we introduce the following two lemmas first. Lemma 3.4.15 shows that with a positive probability, the samples from discrete Gauss distribution are not all contained in a given plane with dimension no more than $n$.

**Lemma 3.4.15** Given an $n$ dimensional lattice $L \subset \mathbb{R}^n$, $\varepsilon \leq \frac{1}{10}$, $r \geq \sqrt{2}\eta_e(L)$, let $H$ be a plane in $\mathbb{R}^n$ with dimension no more than $n - 1$, $x$ be a sample from the discrete Gauss distribution $D_{L,r}$, then

$$\Pr\{x \notin H\} \geq \frac{1}{10}.$$

**Proof** $h = (h_1, h_2, \ldots, h_n) \in H$, without loss of generality, we suppose that $H$ is $h_1 = 0$, i.e. the plane of all points with the first coordinate 0, let $x = (x_1, x_2, \ldots, x_n)$. Consider the expectation $E[e^{-\pi(x_1/r)^2}]$, based on Lemma 1.3.2 in Chap. 1, we have
\[ E_{x \sim D_{L,r}} [e^{-\pi (x_1/r)^2}] \]
\[ = \frac{1}{\rho_r(L)} \sum_{x \in L} e^{-\pi(\sqrt{2}x_1/r)^2} e^{-\pi(x_2/r)^2} \ldots e^{-\pi(x_n/r)^2} \]
\[ = \frac{\det(L^*) r^n}{\sqrt{2} \rho_r(L)} \sum_{y \in L^*} e^{-\pi(r y_1/\sqrt{2})^2} e^{-\pi(r y_2)^2} \ldots e^{-\pi(r y_n)^2} \]
\[ \leq \frac{\det(L^*) r^n}{\sqrt{2} \rho_r(L)} \rho_{\sqrt{2}/r}(L^*), \]

where \( y = (y_1, y_2, \ldots, y_n) \in L^* \). Since \( r/\sqrt{2} \geq \eta_e(L) \), we get
\[ \rho_{\sqrt{2}/r}(L^*) = 1 + \rho_{\sqrt{2}/r}(L^* \setminus \{0\}) \leq 1 + \varepsilon. \]

It follows that
\[ E_{x \sim D_{L,r}} [e^{-\pi (x_1/r)^2}] \leq \frac{\det(L^*) r^n}{\sqrt{2} \rho_r(L)} (1 + \varepsilon). \]

By Lemma 1.3.2 in Chap. 1 again,
\[ \rho_r(L) = \det(L^*) r^n \rho_{1/r}(L^*) \geq \det(L^*) r^n, \]

therefore,
\[ E_{x \sim D_{L,r}} [e^{-\pi (x_1/r)^2}] \leq \frac{1 + \varepsilon}{\sqrt{2}} < \frac{9}{10}. \]

On the other hand,
\[ \sum_{x \in H, x \sim D_{L,r}} \frac{\rho_r(x)}{\rho_r(L)} [e^{-\pi (x_1/r)^2}] = \sum_{x \in H, x \sim D_{L,r}} \frac{\rho_r(x)}{\rho_r(L)} = Pr\{x \in H\}. \]

According to the above two inequalities,
\[ Pr\{x \in H\} \leq \frac{9}{10}, \]

that is,
\[ Pr\{x \notin H\} \geq \frac{1}{10}. \]

The lemma holds. \( \square \)
Based on Lemma 3.4.15, the following lemma shows that it is possible to find $n$ linearly independent vectors from $n^2$ independent samples of the discrete Gauss distribution $D_{L,r}$ with probability close to 1, which provides a guarantee for solving the GIVP problem later.

**Lemma 3.4.16** Given an $n$ dimensional lattice $L \subset \mathbb{R}^n$, $\varepsilon \leq \frac{1}{10}$, $r \geq \sqrt{2} \eta_v(L)$, then the probability that a set of $n^2$ vectors chosen independently from $D_{L,r}$ contain no $n$ linearly independent vectors is exponentially small.

**Proof** Let $x_1, x_2, \ldots, x_{n^2}$ be $n^2$ independent samples from $D_{L,r}$, for $i = 1, 2, \ldots, n-1$, let $B_i$ be the event that

$$\dim \text{span}(x_1, x_2, \ldots, x_{in}) = \dim \text{span}(x_1, x_2, \ldots, x_{(i+1)n}) < n.$$ 

If none of the events $B_1, B_2, \ldots, B_{n-1}$ happens, then

$$\dim \text{span}(x_1, x_2, \ldots, x_{n^2}) = n,$$

i.e. there exists $n$ linearly independent vectors in these $n^2$ samples. Next we estimate the probability of $B_i$, by Lemma 3.4.15,

$$\Pr\{x_j \in \text{span}(x_1, x_2, \ldots, x_{in})\} \leq \frac{9}{10}, \quad \forall \text{ in} + 1 \leq j \leq (i+1)n.$$ 

Thus,

$$\Pr\{x_{in+1}, x_{in+2}, \ldots, x_{(i+1)n} \in \text{span}(x_1, x_2, \ldots, x_{in})\} \leq \left(\frac{9}{10}\right)^{n},$$

that is,

$$\Pr\{B_i\} \leq \left(\frac{9}{10}\right)^{n}, \quad \forall \ i = 1, 2, \ldots, n-1.$$ 

It follows that

$$\Pr\{\overline{B_1} \cap \overline{B_2} \cap \cdots \cap \overline{B_{n-1}}\} = 1 - \Pr\{B_1 \cup \cdots \cup B_{n-1}\} \geq 1 - (n - 1) \left(\frac{9}{10}\right)^{n},$$

this means the probability that none of $B_1, B_2, \ldots, B_{n-1}$ happens is close to 1, i.e. the probability that there are $n$ linearly independent vectors in these $n^2$ independent samples from $D_{L,r}$ is close to 1. We complete the proof. \qed

Based on the above preparations, let’s prove the main conclusion in this subsection.
Lemma 3.4.17 Given an n dimensional lattice $L$, $\varepsilon = \varepsilon(n) \leq \frac{1}{10}$, $\phi(L) \geq \sqrt{2} \eta_\varepsilon(L)$, if there exists an algorithm for the DGSp problem, then there is a probabilistic polynomial algorithm to solve the GIVP$_{2\sqrt{n}\phi}$ problem.

Proof By the LLL algorithm we choose the generated matrix $S = [s_1, s_2, \ldots, s_n]$ of lattice $L$ such that $s_i \leq 2^n \lambda_n(L), 1 \leq i \leq n$. Let

$$\tilde{\lambda}_n = |S| = \max_{1 \leq i \leq n} |s_i|$$

be the length of the longest column vector in $S$, then

$$\lambda_n(L) \leq \tilde{\lambda}_n \leq 2^n \lambda_n(L).$$

For each $i \in \{0, 1, \ldots, 2n\}$, let $r_i = 2^{-i} \tilde{\lambda}_n$, we generate $n^2$ independent samples from $D_{L,r_i}$ based on the algorithm of the DGSp problem, and the corresponding sets of $n^2$ vectors are denoted as $S_0, S_1, \ldots, S_{2n}$. If $\tilde{\lambda}_n \leq \phi(L)$, we have

$$\tilde{\lambda}_n = |S| \leq 2\sqrt{n}\phi(L),$$

so $S$ is a solution of the GIVP$_{2\sqrt{n}\phi}$ problem. If $\phi(L) < \tilde{\lambda}_n$, then there exists $i \in \{0, 1, \ldots, 2n\}$ such that $\phi(L) \leq r_i \leq 2\phi(L)$ according to Lemma 1.3.6 in Chap. 1,

$$\tilde{\lambda}_n \leq 2^n \lambda_n(L) \leq 2^n n^{\frac{\pi}{\ln(1/\varepsilon)}} \eta_\varepsilon(L) < 2^{2n+1} \phi(L),$$

combine $r_0 = \tilde{\lambda}_n > \phi(L)$ with $r_{2n} = 2^{-2n} \tilde{\lambda}_n < 2\phi(L)$, we know there is $r_i$ satisfying $\phi(L) \leq r_i \leq 2\phi(L)$. By Lemma 3.4.16, the probability that $S_i$ contains $n$ linearly independent vectors $v_1, v_2, \ldots, v_n$ is close to 1. Based on Lemma 1.3.4 in Chap. 1, the probability each $v_i$ no more than $\sqrt{n}r_i \leq 2\sqrt{n}\phi(L)$ is close to 1. Let $V = [v_1, v_2, \ldots, v_n]$, we get $|V| \leq 2\sqrt{n}\phi(L)$, so we find a solution of the GIVP$_{2\sqrt{n}\phi}$ problem. This lemma holds. \qed

In Chap. 2, we have proved that the hard problems on lattice such as the GIVP and GapSIVP problems can be reduced to the SIS problem, so the difficulties of solving the hard problems on lattice are the same. In Lemma 3.4.17, we prove that if there is an algorithm for the DGSp problem, then there is a probabilistic polynomial algorithm to solve the GIVP problem with positive probability, which can also solve the other hard problems on lattice. So far we have completed the second part of the proof of Theorem 3.3.1. In the first part, we have proved that if there is an algorithm for the LWE problem, then there exists a quantum algorithm to solve the DGSp problem. Combining the two parts of the proof, we get the feasibility to solve the hard problems on lattice based on the algorithm for solving the LWE problem, that is, the difficulty of solving the LWE problem is not lower than that of the hard problems on lattice.
3.4.3 From D-LWE to LWE

In this subsection, we will finish the third part of the proof for Theorem 3.3.1, i.e. the difficulty of the D-LWE problem is at least as high as that of the LWE problem, which is given in the following Theorem 3.4.1.

**Theorem 3.4.1** Let $n \geq 1$ be a positive integer, $2 \leq q \leq \text{Poly}(n)$ be a prime number, $\chi$ be a distribution on $\mathbb{Z}_q$. Assume that we have an algorithm $W$ to determine a sample from the LWE distribution $A_{s,\chi}$ or the uniform distribution $U$ with probability close to 1, then there exists an algorithm $W'$ to solve $s$ given some samples from the LWE distribution $A_{s,\chi}$ with probability close to 1.

**Proof** Let $s = (s_1, s_2, \ldots, s_n) \in \mathbb{Z}_q^n$, we give the steps for solving $s_1$ of the algorithm $W'$, and $s_2, \ldots, s_n$ could be solved in the same way. For $k \in \mathbb{Z}_q$, consider the following transformation of the LWE sample $(a, b)$, where $a$ is uniformly distributed on $\mathbb{Z}_q^n$, $b = a \cdot s + e$, $e \leftarrow \chi$,

$$(a, b) \longrightarrow (a + (l, 0, \ldots, 0), b + lk),$$

here $l \in \mathbb{Z}_q$ is uniformly distributed. If $k = s_1$, then

$$b + lk = a \cdot s + e + ls_1 = (a + (l, 0, \ldots, 0)) \cdot s + e,$$

note that $a + (l, 0, \ldots, 0)$ is also uniform on $\mathbb{Z}_q^n$, therefore, $(a + (l, 0, \ldots, 0), b + lk)$ has the LWE distribution $A_{s,\chi}$.

On the other hand, if $k \neq s_1$, at this time $lk$ and $b$ are independent, based on $l$ is uniform on $\mathbb{Z}_q$, it follows that $lk$ is also uniform on $\mathbb{Z}_q$. By Lemma 3.3.2, we get $b + lk$ is uniform on $\mathbb{Z}_q$, so $(a + (l, 0, \ldots, 0), b + lk)$ is uniform. By the algorithm $W$, we determine $(a + (l, 0, \ldots, 0), b + lk)$ is from the LWE distribution $A_{s,\chi}$ or the uniform distribution, and check whether $s_1$ is equal to $k$. Since the number of possible values of $k$ is $q$, we can always find the solution of $s_1$. After solving $s_2, s_3, \ldots, s_n$ in the same way, we get the solution $s$. The lemma holds. □

In Theorem 3.4.1, we prove that the difficulty of the D-LWE problem is not lower than that of the LWE problem and complete the whole proof of Theorem 3.3.1. The difficulty from solving the D-LWE problem to the LWE problem, then to the hard problems on lattice does not increase. We will further discuss the LWE cryptosystem with the probability of decryption error in the next chapter.
Open Access  This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.