Financial Mathematics and Fintech

Zhiyong Zheng
Kun Tian
Fengxia Liu

# Modern Cryptography Volume 2

## A Classical Introduction to Informational and Mathematical Principle

OPEN ACCESS

Springer

# Financial Mathematics and Fintech

This series addresses the emerging advances in mathematical theory related to finance and application research from all the fintech perspectives. It is a series of monographs and contributed volumes focusing on the in-depth exploration of financial mathematics such as applied mathematics, statistics, optimization, and scientific computation, and fintech applications such as artificial intelligence, block chain, cloud computing, and big data. This series is featured by the comprehensive understanding and practical application of financial mathematics and fintech. This book series involves cutting-edge applications of financial mathematics and fintech in practical programs and companies.

The Financial Mathematics and Fintech book series promotes the exchange of emerging theory and technology of financial mathematics and fintech between academia and financial practitioner. It aims to provide a timely reflection of the state of art in mathematics and computer science facing to the application of finance. As a collection, this book series provides valuable resources to a wide audience in academia, the finance community, government employees related to finance and anyone else looking to expand their knowledge in financial mathematics and fintech.

The key words in this series include but are not limited to:
a) Financial mathematics
b) Fintech
c) Computer science
d) Artificial intelligence
e) Big data

Zhiyong Zheng · Kun Tian · Fengxia Liu

# Modern Cryptography Volume 2

## A Classical Introduction to Informational and Mathematical Principle

Springer

Zhiyong Zheng
School of Mathematics
Renmin University of China
Beijing, China

Henan Academy of Sciences
Zhengzhou, China

Kun Tian
School of Mathematics
Renmin University of China
Beijing, China

Fengxia Liu
Artificial Intelligence Research Institute
Beihang University
Beijing, China

ISSN 2662-7167 ISSN 2662-7175 (electronic)
Financial Mathematics and Fintech
ISBN 978-981-19-7643-8 ISBN 978-981-19-7644-5 (eBook)
https://doi.org/10.1007/978-981-19-7644-5



This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

# Preface

For integer factorization and discrete logarithm calculation, P.W.Shor published an effective quantum calculation in *SIAM Journal on Computing* in 1997, which is called the Shor algorithm in academic circles. Classical public key cryptosystems such as RSA, ECC and so on could not resist the attack of the Shor algorithm, so the major security risks of public key cryptosystems are completely exposed to the Shor algorithm and quantum computer.

In the past 20 years, the rise and development of post-quantum cryptography have close relation with the lattice cryptosystems. The academic community believes that the hard problems on lattice, such as the shortest vector problem (SVP), the continuous shortest vector problem (SIVP) and the determination of the shortest vector problem (GapSVP) can resist quantum computing effectively, so the public key cryptosystems based on the hard problems on lattice become the core theory and technology of the post-quantum cryptography. At present, there are six kinds of published post-quantum cryptosystems:

1. Ajtai-Dwork cryptosystem (1997). Ajtai constructed a collision-resistant Hash function by the circulant matrix and ideal matrix, and converted the collision point into the shortest vector problem on $q$-ary integer lattice. Ajtai first proposed the concept of random lattice (Gauss lattice) in 1996, and established the famous reduction principle 'from the worst case to the average case'. The security of Ajtai-Dwork cryptosystem could be fully proved by this reduction principle.
2. GGH/HNF cryptosystem (1997). In 1997, Goldereich, Goldwasser and Halevi constructed a public key cryptosystem based on the closest vector problem on the $q$-ary integer lattice, which was further improved by Micciancio using the Hermite normal basis in 2005. The idea of Micciancio is very simple. Since the HNF basis of any lattice can be easily computed from its generated matrix, the GGH cryptosystem uses the HNF basis as the public key directly.
3. NTRU cryptosystem (1998). Number Theory Research Unit (NTRU) is a quantum-resistant computing public key cryptosystem developed by J. Hoffstein, J. Pipher and J. H. Silverman in Brown University in 1998, which has become the most attractive post-quantum cryptosystem due to its simple algorithm, fast

calculation speed and small storage space. In 2009, the National Institute of Standards and Technology wrote a survey report: there is no cryptosystem could consider both public key encryption and digital signature, and resist the Shor algorithm simultaneously. The NTRU encryption algorithm seems to be the most likely choice among many lattice-based encryption schemes. The PQCRYPTO program (Horizon 2020 ICT-645622) by European Union hopes to develop a new European encryption standard based on the NTRU improved by Stehle-Steinfeld.

4. MacElience/Niderreiter cryptosystem (1998). Linear codes are the earliest error-correcting codes in coding theory. Later, algebraic coding developed based on the ideal theory greatly enriched and improved the linear coding theory. Cycle code and Goppa code are the most important error-correcting codes in algebraic coding. MacElience and Niderreiter constructed a new public key cryptosystem by using the asymmetry of encoding algorithm and decoding algorithm of the error-correcting code independently, which we call MacElience/Niderreiter cryptosystem. Since a code (linear code or algebraic code) can be regarded as a lattice on a finite field, the security of this cryptosystem is closely related to the closest vector problem on the $q$-ary integer lattice. Recent studies have shown that coding theory plays an important role in lattice-based cryptosystems.
5. LWE cryptosystem (2005). In 2005, O. Regev of Tel Aviv University in Israel proposed the famous LWE cryptosystem based on the LWE distribution. Because of this work, Regev won the highest award in the theoretical computer science in 2018—the Godel Award. The LWE distribution (Learning With Errors) is a random linear system with errors having Gauss distribution. Regev's cryptosystem encrypts a single bit of plaintext each time. Since the security of the LWE problem has been clearly proved (see Chap. 3 of this book), LWE cryptosystem is currently the most active and mainstream research topic.
6. Fully homomorphic encryption (FHE). In 1985, R.Rivest, C.Adleman and M.Dertouzos first proposed the concept of data bank and the conjecture of fully homomorphic encryption. Some individuals and organizations encrypt the original data and store them in the data bank for privacy protection, which is obviously a huge wealth. How to compute these encrypted data effectively? R. Rivest, C. Adleman and M. Dertouzos presented the fully homomorphic encryption conjecture. In 2009, C. Gentry of Stanford University partially solved the RAD conjecture. Gentry's work is based on the ideal lattice, that is, an integer lattice which has a one-to-one correspondence to the ideal of polynomial ring. But the cryptosystem of Gentry is a finite-time fully homomorphic encryption, and infinite fully homomorphic encryption is still an unsolved public problem. In 2012 and 2013, the second and third fully homomorphic encryption algorithms based on the LWE distribution were proposed one after another. Gentry won the 2022 Godel Award for his contributions.

In the book *Modern Cryptography*, we give a detailed introduction to the basic theory of lattice and the first four kinds of lattice-based cryptosystems. The main purpose of this book is to discuss the computational complexity theory of lattice

cryptosystems, especially Ajtai's reduction principle, and fill the gap that post-quantum cryptography focuses on the encryption and decryption algorithms, and the theoretical proof is insufficient. In Chaps. 3, 4 and 6, we introduce the LWE distribution, LWE cryptosystem and fully homomorphic encryption in detail. When using stochastic analysis tools, there are many 'ambiguity' problems in terms of definitions and algorithms, such as the '$\approx$' notation appeared in a large number of papers and books, which is unprecise mathematically. The biggest characteristic of this book is to use probability distribution to provide rigorous mathematical definitions and proofs for various unclear expressions, making it a rigorous theoretical system to facilitate teaching and dissemination in class. Chapters 5 and 7 are based on two papers published by the authors in the journal *Journal of Information Security* (see references [63, 64]). These materials can be regarded as some important topics, such as the further extension and improvement of cyclic lattices, ideal lattices and generalized NTRU cryptosystems.

This book contains the most cutting-edge and hottest research topics in post-quantum cryptography. Reading all the chapters requires a lot of mathematical knowledge and a good mathematical foundation. Therefore, this book can be used as a textbook for graduate students in mathematics and cryptography, or a reference book for researchers in cryptography area. Due to the rush of time, all the materials are summarized from domestic and foreign research papers in the last 20 years, and shortcomings and mistakes are inevitable. We welcome readers to criticize and correct them.

Zhengzhou, China
September 2022

Zhiyong Zheng

# Contents

# Notations

| | |
|---|---|
| $\mathbb{R}^n$ | $n$ dimensional Euclidean space |
| $\mathbb{Z}^n$ | Integer points in $\mathbb{R}^n$ |
| $\mathbb{Z}_q$ | Residue class ring mod $q$ |
| $\mathbb{C}$ | Complex field |
| $\mathbb{R}[x]$ | Polynomial ring of one variable on $\mathbb{R}$ |
| $\mathbb{Z}[x]$ | Polynomial ring of one variable on $\mathbb{Z}$ |
| $\mathbb{Z}_q[x]$ | Polynomial ring of one variable on $\mathbb{Z}_q$ |
| $\|x\|$ | $l_2$ norm of vector $x$ |
| $N(x_0, r)$ | Sphere with center $x_0$ and radius $r$ in $\mathbb{R}^n$ |
| $[a]$ | The largest integer no more than real number $a$ |
| $\{a\}$ | The fractional part of real number $a$ |
| $\lfloor a \rceil$ | The nearest integer to real number $a$ |
| $\hat{f}$ | Fourier transform of function $f$ |
| $\Delta(\xi, \eta)$ | Statistical distance of random variable $\xi$ and $\eta$ |
| $E(\xi)$ | Expectation of random variable $\xi$ |
| $Var(\xi)$ | Variance of random variable $\xi$ |
| $Pr\{A\}$ | Probability of random event $A$ |
| $U(G)$ | Uniform distribution on $G$ |
| $\Phi(x)$ | Cumulative distribution of standard normal distribution |
| $\mathrm{poly}(n)$ | Polynomial function of $n$ |
| $L = L(B)$ | Lattice $L$ with generated matrix $B$ |
| $L(B)^{\perp}$ | Dual lattice of $L$ with generated matrix $(B^T)^{-1}$ |
| $F(B)$ | Basic neighborhood of lattice with generated matrix $B$ |
| $\lambda_1(L)$ | Minimal distance of lattice $L$ |
| $\rho(L)$ | Covering radius of lattice $L$ |
| $\eta_\epsilon(L)$ | Smoothing parameter of lattice $L$ |
| $a\|x\rangle$ | Product of real number $a$ and vector $x$ |
| $x \cdot y$ | Inner product of vector $x$ and $y$ |
| $A \otimes B$ | Kronecker product of matrix $A$ and $B$ |
| $\epsilon(n)$ | Negligible function of $n$ |
| $g(n) = \tilde{O}(f(n))$ | $g(n) = O(f(n)\mathrm{loglog}\|f(n)\|)$ |

# Chapter 1
# Random Lattice Theory


Let $\mathbb{R}^n$ be the Euclidean space of dimension $n, x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ are two vectors of $\mathbb{R}^n$, the inner product of $x$ and $y$ is defined as

$$x \cdot y = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = x^{\mathrm{T}} y. \tag{1.0.1}$$

The Euclidean norm $|x|$ of vector $x$ (also called the $l_2$ norm) is defined as

$$|x| = (x_1^2 + x_2^2 + \cdots + x_n^2)^{\frac{1}{2}} = \sqrt{x \cdot x}. \tag{1.0.2}$$

Let $B = (b_{ij})_{n\times n} \in \mathbb{R}^{n\times n}$ be an invertible square matrix of order $n$, a full-rank lattice $L$ in $R^n$ is defined as

$$L = L(B) = \{Bx \mid x \in \mathbb{Z}^n\}. \tag{1.0.3}$$

A lattice $L$ is a discrete geometry in $\mathbb{R}^n$, in other words, there is a positive constant $\lambda_1 = \lambda_1(L) > 0$ and a vector $\alpha \in L$ satisfying $\alpha \neq 0$, such that

$$|\alpha| = \min_{x\in L, x\neq 0} |x| = \lambda_1(L). \tag{1.0.4}$$

$\lambda_1$ is called the shortest distance in $L$, $\alpha$ is the shortest vector in $L$. A sphere in $n$ dimensional Euclidean space $\mathbb{R}^n$ with center $x_0$ and radius $r$ is defined as

$$N(x_0, r) = \{x \in \mathbb{R}^n \mid |x - x_0| \leqslant r\},\ x_0 \in \mathbb{R}^n. \tag{1.0.5}$$



Z. Zheng et al., *Modern Cryptography Volume 2*, Financial Mathematics and Fintech,
https://doi.org/10.1007/978-981-19-7644-5_1

In particular, $N(0, r)$ represents a sphere with origin as the center of the circle and radius $r$. The discretization of a lattice is equivalent to the fact that the intersection of $L$ with any sphere $N(x_0, r)$ is a finite set, i.e.

$$^{\#}\{L \cap N(x_0, r)\} < \infty. \tag{1.0.6}$$

Let $L = L(B)$ be a lattice, $B$ is the generated matrix of $L$. Block $B$ by each column vector as $B = [\beta_1, \beta_2, \ldots, \beta_n]$, the basic neighborhood $F(B)$ of $L$ is defined as

$$F(B) = \{\sum_{i=1}^{n} x_i \beta_i \mid 0 \leqslant x_i < 1\}. \tag{1.0.7}$$

Clearly the basic neighborhood $F(B)$ is related to the generated matrix $B$ of $L$, which is actually a set of representative elements of the additive quotient group $\mathbb{R}^n/L$. $F^*(B)$ is also a set of representative elements of the quotient group $\mathbb{R}^n/L$, where

$$F^*(B) = \{\sum_{i=1}^{n} x_i \beta_i \mid -\frac{1}{2} \leqslant x_i < \frac{1}{2}\},$$

therefore, $F^*(B)$ can also be a basic neighborhood of the lattice $L$. The following property is easy to prove [see Lemma 2.6 in Chap. 7 in Zheng (2022)]

$$\mathrm{Vol}(F(B)) = |\det(B)| = \det(L). \tag{1.0.8}$$

That is, the volume of the basic neighborhood of $L$ is an invariant and does not change with the choice of the generated matrix $B$. We denote $\det(L) = |\det(B)|$ as the determinant of the lattice $L$.

The basic properties of lattice can be found in Chap. 7 of Zheng (2022). The main purpose of this chapter is to establish the random theory of lattice. If a lattice $L$ is the space of values of a random variable (or random vector), it is called a random lattice. Random lattice is a new research topic in lattice theory, and the works of Micciancio and Regev (2004), Regev (2004), Micciancio and Regev (2004), Micciancio and Regev (2009) are pioneering. In this way, the study of random lattice is no more than ten years. For technical reasons, only a special class of random lattices can be defined and studied. That is, consider a random variable $\xi$ defined in $\mathbb{R}^n$ from a Gauss distribution, and limit the discretization of $\xi$ to $L$ so that $L$ becomes a random lattice. It is a special kind of random lattice, which we call the Gauss lattice. The main purpose of this chapter is to introduce Gauss lattice, define the smoothing parameter on Gauss lattice and calculate the statistical distance based on the smoothing parameter. The mathematical technique used in this chapter is high dimensional Fourier transform.

## 1.1 Fourier Transform

A complex function $f(x)$ on $\mathbb{R}^n$ is a mapping of $\mathbb{R}^n \to \mathbb{C}$, where $\mathbb{C}$ is the complex field. We define the function space $L^1(\mathbb{R})$ and $L^2(\mathbb{R})$:

$$L^1(\mathbb{R}) = \{f : \mathbb{R}^n \to \mathbb{C} \mid \int_{\mathbb{R}^n} |f(x)|\mathrm{d}x < \infty\} \tag{1.1.1}$$

and

$$L^2(\mathbb{R}) = \{f : \mathbb{R}^n \to \mathbb{C} \mid \int_{\mathbb{R}^n} |f(x)|^2\mathrm{d}x < \infty\}. \tag{1.1.2}$$

If $f(x), g(x) \in L^1(\mathbb{R}^n)$, define the convolution of $f$ with $g$ as

$$f * g(x) = \int_{\mathbb{R}^n} f(x-\xi)g(\xi)\mathrm{d}\xi. \tag{1.1.3}$$

We have the following properties about convolution.

**Lemma 1.1.1** *Suppose $f(x), g(x) \in L^1(\mathbb{R}^n)$, then*
*(i) $f * g(x) = g * f(x)$.*
*(ii) $\int_{\mathbb{R}^n} f * g(x)\mathrm{d}x = \int_{\mathbb{R}^n} f(x)\mathrm{d}x \cdot \int_{\mathbb{R}^n} g(x)\mathrm{d}x$.*

***Proof*** By the definition of convolution (1.1.3), we have

$$g * f(x) = \int_{\mathbb{R}^n} g(x-\xi)f(\xi)\mathrm{d}\xi = \int_{\mathbb{R}^n} g(y)f(x-y)\mathrm{d}y = f * g(x).$$

Property (i) holds. To obtain the second result (ii), we have

$$\int_{\mathbb{R}^n} f * g(x)\mathrm{d}x = \int_{\mathbb{R}^n} (\int_{\mathbb{R}^n} f(x-\xi)g(\xi)\mathrm{d}\xi)\mathrm{d}x$$

$$= \int_{\mathbb{R}^n}\int_{\mathbb{R}^n} f(y)g(\xi)\mathrm{d}y\mathrm{d}\xi = \int_{\mathbb{R}^n} f(y)\mathrm{d}y \cdot \int_{\mathbb{R}^n} g(\xi)\mathrm{d}\xi.$$

The lemma is proved. □

**Definition 1.1.1** If $f(x) \in L^1(\mathbb{R}^n)$, define the Fourier transform of $f(x)$ as

$$\hat{f}(x) = \int_{\mathbb{R}^n} f(\xi) \mathrm{e}^{-2\pi i x\cdot\xi} \mathrm{d}\xi, \ x \in \mathbb{R}^n. \tag{1.1.4}$$

Note that $f \to \hat{f}$ is an operator of the function space defined on $L^1(\mathbb{R}^n)$, which is called the Fourier operator. If $f(x) = f_1(x_1) f_2(x_2) \cdots f_n(x_n)$, then the high dimensional Fourier operator can be reduced to the product of one dimensional Fourier operators, i.e.

$$\hat{f}(x) = \Pi_{i=1}^n \hat{f}_i(x_i). \tag{1.1.5}$$

The following are some of the most common and fundamental properties of Fourier transform.

**Lemma 1.1.2** *Suppose $f(x) \in L^1(\mathbb{R}^n)$, $g(x) \in L^1(\mathbb{R}^n)$, then*
*(i) $\widehat{f * g}(x) = \hat{f}(x)\hat{g}(x)$.*
*(ii) $a \in \mathbb{R}^n$ is a given vector, denote $\tau_a f$ as the coordinate translation function, i.e. $\tau_a f(x) = f(x + a)$, $\forall x \in \mathbb{R}^n$. Then we have $\widehat{\tau_a f}(x) = e^{2\pi i x\cdot a}\hat{f}(x)$.*
*(iii) Let $h(x) = e^{2\pi i x\cdot a} f(x)$, thus $\hat{h}(x) = \hat{f}(x - a)$.*
*(iv) Let $\delta \neq 0$ be he real number, $f_\delta(x) = f(\frac{1}{\delta}x)$, then $\hat{f}_\delta(x) = |\delta|^n \hat{f}_{\delta^{-1}}(x) = |\delta|^n \hat{f}(\delta x)$.*
*(v) Let $A$ be an invertible real matrix of order n, namely $A \in GL_n(\mathbb{R})$, define $f \circ A(x) = f(Ax)$. Then $\widehat{f \circ A}(x) = |A|^{-1}\hat{f} \circ (A^{-1})^T(x) = |A|^{-1}\hat{f}((A^{-1})^T x)$, where $A^T$ is the transpose matrix of $A$.*

***Proof*** By definition, we have

$$\widehat{f * g}(x) = \int_{\mathbb{R}^n} f * g(\xi) \mathrm{e}^{-2\pi i x\cdot\xi} \mathrm{d}\xi$$

$$= \int_{\mathbb{R}^n} \Big( \int_{\mathbb{R}^n} f(\xi - y) g(y) \mathrm{d}y \Big) \mathrm{e}^{-2\pi i x\cdot\xi} \mathrm{d}\xi.$$

Taking variable substitution $\xi - y = y'$, then $\xi = y + y'$, and $\mathrm{d}\xi = \mathrm{d}y'$, so we have

$$\widehat{f * g}(x) = \int_{\mathbb{R}^n} g(y) \mathrm{e}^{-2\pi i x\cdot y} \mathrm{d}y \cdot \int_{\mathbb{R}^n} f(y') \mathrm{e}^{-2\pi i x\cdot y'} \mathrm{d}y' = \hat{f}(x)\hat{g}(x),$$

property (i) is proved. Based on the definition of Fourier transform, we have

$$\widehat{\tau_a f}(x) = \int_{\mathbb{R}^n} f(\xi + a)\mathrm{e}^{-2\pi i x\cdot\xi}\mathrm{d}\xi = \int_{\mathbb{R}^n} f(y)\mathrm{e}^{-2\pi i x\cdot(y-a)}\mathrm{d}y$$

$$= \mathrm{e}^{2\pi i x\cdot a}\int_{\mathbb{R}^n} f(y)\mathrm{e}^{-2\pi i x\cdot y}\mathrm{d}y = \mathrm{e}^{2\pi i x\cdot a}\hat{f}(x),$$

property (ii) gets proved. Similarly, we can obtain (iii). Next, we give the proof of (iv). Since $\delta \neq 0$, and $f_\delta(x) = f(\frac{1}{\delta}x)$, so

$$\hat{f}_\delta(x) = \int_{\mathbb{R}^n} f(\frac{1}{\delta}\xi)\mathrm{e}^{-2\pi i x\cdot\xi}\mathrm{d}\xi = \int_{\mathbb{R}^n} f(y)\mathrm{e}^{-2\pi i x\cdot\delta y}|\delta|^n\mathrm{d}y$$

$$= \int_{\mathbb{R}^n} f(y)\mathrm{e}^{-2\pi i(\delta x\cdot y)}|\delta|^n\mathrm{d}y = |\delta|^n\hat{f}_{\delta^{-1}}(x).$$

By the condition $A \in GL_n(\mathbb{R})$, $f\circ A(x) = f(Ax)$, then

$$\widehat{f\circ A}(x) = \int_{\mathbb{R}^n} f(A\xi)\mathrm{e}^{-2\pi i x\cdot\xi}\mathrm{d}\xi.$$

Taking variable substitution, $y = A\xi$, then $A^{-1}y = \xi$, and $\mathrm{d}\xi = |A|^{-1}\mathrm{d}y$, so

$$\widehat{f\circ A}(x) = \int_{\mathbb{R}^n} f(y)\mathrm{e}^{-2\pi i x\cdot A^{-1}y}|A|^{-1}\mathrm{d}y = |A|^{-1}\int_{\mathbb{R}^n} f(y)\mathrm{e}^{-2\pi i((A^{-1})^{\mathrm{T}}x\cdot y)}\mathrm{d}y$$

$$= |A|^{-1}\hat{f}((A^{-1})^{\mathrm{T}}x) = |A|^{-1}\hat{f}\circ(A^{-1})^T(x).$$

Lemma 1.1.2 is proved. □

Finally, we give some examples of the Fourier transform.

***Example 1.1*** Let $n = 1$, $a \in \mathbb{R}$, $a > 0$, define the characteristic function $1_{[-a,a]}(x)$ of the closed interval $[-a, a]$ as

$$1_{[-a,a]}(x) = \begin{cases} 1, & x \in [-a, a], \\ 0, & x \notin [-a, a]. \end{cases}$$

Then

$$\hat{1}_{[-a,a]}(x) = \frac{\sin 2\pi a x}{\pi x}. \tag{1.1.6}$$

For $n > 1$, let $a = (a_1, a_2, \ldots, a_n) \in \mathbb{R}^n$, the square $[-a, a]$ is defined as

$$[-a, a] = [-a_1, a_1] \times [-a_2, a_2] \times \cdots \times [-a_n, a_n].$$

Define the characteristic function $1_{[-a,a]}(x)$ of the square $[-a, a]$, then

$$\hat{1}_{[-a,a]}(x) = \Pi_{i=1}^{n} \frac{\sin 2\pi a_i x_i}{\pi x_i}. \tag{1.1.7}$$

***Proof*** For the general $n$, it is clear that

$$1_{[-a,a]}(x) = \Pi_{i=1}^{n} 1_{[-a_i,a_i]}(x_i).$$

Based on Eq. (1.1.5), we only need to prove Eq. (1.1.6). $n = 1$, $a \in \mathbb{R}$, so

$$\hat{1}_{[-a,a]}(x) = \int_{\mathbb{R}} 1_{[-a,a]}(\xi) \mathrm{e}^{-2\pi i x \xi} \mathrm{d}\xi = \int_{-a}^{a} \mathrm{e}^{-2\pi i x \xi} \mathrm{d}\xi = \frac{1}{\pi x} \sin 2\pi a x.$$

□

***Example 1.2*** Let $f(x) = \mathrm{e}^{-\pi |x|^2}$, $x \in \mathbb{R}^n$, then $f(x) \in L^1(\mathbb{R}^n)$, and $\hat{f}(x) = f(x)$, namely $f(x)$ is a fixed point of Fourier operator, which is also called a dual function.

***Proof*** Clearly, $f(x) \in L^1(\mathbb{R}^n)$. To prove the fixed point property of $f(x)$, by definition

$$\hat{f}(x) = \int_{\mathbb{R}^n} \mathrm{e}^{-\pi |\xi|^2 - 2\pi i x \cdot \xi} \mathrm{d}\xi = \mathrm{e}^{-\pi |x|^2} \int_{\mathbb{R}^n} \mathrm{e}^{-\pi |\xi + i x|^2} \mathrm{d}\xi = \mathrm{e}^{-\pi |x|^2} \int_{\mathbb{R}^n} \mathrm{e}^{-\pi |y|^2} \mathrm{d}y.$$

By one dimensional Poisson integral,

$$\int_{-\infty}^{+\infty} \mathrm{e}^{-\pi y^2} \mathrm{d}y = 1, \tag{1.1.8}$$

we have the following high dimensional Poisson integral,

$$\int_{\mathbb{R}^n} \mathrm{e}^{-\pi |y|^2} \mathrm{d}y = 1. \tag{1.1.9}$$

So we get $\hat{f}(x) = f(x)$. □

## 1.2 Discrete Gauss Measure

From the property of $f(x) = \mathrm{e}^{-\pi|x|^2}$ under the Fourier operator introduced in the last section, and high dimensional Poisson integral formula (1.1.9), we can generalize $f(x)$ as the density function of a random variable from the normal Gauss distribution to a general Gauss distribution in $\mathbb{R}^n$. We first discuss the Gauss function on $\mathbb{R}^n$.

**Definition 1.2.1** Let $s > 0$ be a given positive real number, $c \in \mathbb{R}^n$ is a vector. The Gauss function $\rho_{s,c}(x)$ centered on $c$ with parameter $s$ is defined as

$$\rho_{s,c}(x) = \mathrm{e}^{-\frac{\pi}{s^2}|x-c|^2}, \ x \in \mathbb{R}^n \tag{1.2.1}$$

and

$$\rho_s(x) = \rho_{s,0}(x), \ \rho(x) = \rho_1(x) = \mathrm{e}^{-\pi|x|^2}. \tag{1.2.2}$$

From the definition we have

$$\rho_s(x) = \rho(\frac{1}{s}x) = \mathrm{e}^{-\pi|\frac{x}{s}|^2}$$

and

$$\rho_s(x) = \rho_s(x_1)\ldots\rho_s(x_n).$$

It can be obtained from Poisson integral formula (1.1.9)

$$\int\limits_{\mathbb{R}^n} \rho_s(x)\mathrm{d}x = \int\limits_{\mathbb{R}^n} \rho_{s,c}(x)\mathrm{d}x = s^n. \tag{1.2.3}$$

**Lemma 1.2.1** *The Fourier transform of Gauss functions $\rho_s(x)$ and $\rho_{s,c}(x)$ are*

$$\hat{\rho}_s(x) = s^n\rho_{1/s}(x) = s^n e^{-\pi|sx|^2} \tag{1.2.4}$$

*and*

$$\hat{\rho}_{s,c}(x) = e^{-2\pi ix\cdot c}s^n\rho_{1/s}(x). \tag{1.2.5}$$

***Proof*** By property (iv) of Lemma 1.1.2 and $s > 0$, we have

$$\hat{\rho}_s(x) = s^n\hat{\rho}_{1/s}(x) = s^n\hat{\rho}(sx) = s^n\rho(sx).$$

The last equation follows from Example 2 in the previous section, therefore, (1.2.4) holds. By the property (ii) of Lemma 1.1.2, we have

$$\hat{\rho}_{s,c}(x) = \widehat{\tau_{-c}\rho_s}(x) = \mathrm{e}^{-2\pi ix\cdot c}\hat{\rho}_s(x) = s^n\mathrm{e}^{-2\pi ix\cdot c}\rho_{1/s}(x).$$

Lemma 1.2.1 is proved. □

**Lemma 1.2.2** *$\rho_{s,c}(x)$ is uniformly continuous in $\mathbb{R}^n$, i.e. for any $\epsilon > 0$, there is $\delta = \delta(\epsilon)$, when $|x - y| < \delta$ for $x \in \mathbb{R}^n$, $y \in \mathbb{R}^n$, we have*

$$|\rho_{s,c}(x) - \rho_{s,c}(y)| < \epsilon.$$

***Proof*** By definition, $0 < \rho_{s,c}(x) \leqslant 1$, hence $\rho_{s,c}(x)$ is uniformly bounded in $\mathbb{R}^n$, we will prove $\rho_{s,c}^{'}(x)$ is also uniformly bounded in $\mathbb{R}^n$. We only prove the case of $c = 0$. Since $\rho_s(x) = \rho_s(x_1) = \cdots = \rho_s(x_n)$, without loss of generality, let $n = 1$, $t \in \mathbb{R}$, then

$$\rho_s^{'}(t) = -\frac{2\pi}{s^2} t \mathrm{e}^{-\frac{\pi}{s^2}t^2}.$$

When $|t| \geqslant M$, it is clear

$$\mathrm{e}^{-\frac{\pi}{s^2}t^2} \leqslant \frac{1}{|t|^2}.$$

Hence, when $|t| \geqslant M$, we have

$$|\rho_s^{'}(t)| \leqslant \frac{2\pi}{s^2|t|} \leqslant \frac{2\pi}{s^2 M}.$$

For $|t| < M$, By the continuity of $\rho_s^{'}(t)$ we have $\rho_s^{'}(t)$ is bounded. This gives the proof that $\rho_{s,c}^{'}(x)$ is uniformly continuous in $\mathbb{R}^n$. Let $|\rho_{s,c}^{'}(x)| \leqslant M_0, \forall x \in \mathbb{R}^n$. By the differential mean value theorem, we have

$$|\rho_{s,c}(x) - \rho_{s,c}(y)| = |\rho_{s,c}^{'}(\xi)| \cdot |x - y| \leqslant M_0|x - y|.$$

Let $\delta = \frac{\epsilon}{M_0}$, then

$$|\rho_{s,c}(x) - \rho_{s,c}(y)| < \epsilon, \quad \text{if } |x - y| < \delta.$$

We finish the proof of the lemma. □

**Definition 1.2.2** For $s > 0$, $c \in \mathbb{R}^n$, define the continuous Gauss density function $D_{s,c}(x)$ as

$$D_{s,c}(x) = \frac{1}{s^n}\rho_{s,c}(x), \quad \forall x \in \mathbb{R}^n. \tag{1.2.6}$$

The definition gives that

$$\int_{\mathbb{R}^n} D_{s,c}(x)\mathrm{d}x = \frac{1}{s^n}\int_{\mathbb{R}^n} \rho_{s,c}(x)\mathrm{d}x = 1.$$

Thus, a continuous Gauss density function $D_{s,c}(x)$ corresponds to a continuous random vector of from Gauss distribution in $\mathbb{R}^n$, and this correspondence is one-to-one.

**Definition 1.2.3** Suppose $f(x) : \mathbb{R}^n \to \mathbb{C}$ is an $n$-elements function, $A \subset \mathbb{R}^n$ is a finite or countable set in $\mathbb{R}^n$, define $f(A)$ as

$$f(A) = \sum_{x \in A} f(x). \tag{1.2.7}$$

The continuous Gauss density function $D_{s,c}(x)$ is also called the continuous Gauss measure. In order to implement the transformation from continuous measure to discrete measure and define random variables on discrete geometry in $\mathbb{R}^n$, the following lemma is an important theoretical support.

**Lemma 1.2.3** *Let $L \subset \mathbb{R}^n$ be a full-rank lattice, then*

$$D_{s,c}(L) = \sum_{x \in L} D_{s,c}(x) < \infty.$$

***Proof*** From definition,

$$D_{s,c}(L) = \frac{1}{s^n} \sum_{x \in L} \rho_{s,c}(x) = \frac{1}{s^n} \sum_{x \in L} \mathrm{e}^{-\frac{\pi}{s^2}|x-c|^2}.$$

By the property of the exponential function $\mathrm{e}^t$, there exists a constant $M_0 > 0$, when $|x - c| > M_0$,

$$\mathrm{e}^{-\frac{\pi}{s^2}|x-c|^2} \leqslant \frac{s^2}{\pi |x - c|^2}. \tag{1.2.8}$$

Thus, we can divide the points on the lattice $L$ into two sets. Let

$$A_1 = L \cap \{x \in \mathbb{R}^n \mid |x - c| \leqslant M_0\} = L \cap N(c, M_0).$$

and

$$A_2 = L \cap \{x \in \mathbb{R}^n \mid |x - c| > M_0\}.$$

From (1.0.6) we have

$$\sum_{x \in A_1} \mathrm{e}^{-\frac{\pi}{s^2}|x-c|^2} \leqslant \sum_{x \in A_1} 1 =^{\#} A_1 < \infty.$$

Based on (1.2.8),

$$\sum_{x \in A_2} \mathrm{e}^{-\frac{\pi}{s^2}|x-c|^2} \leqslant \sum_{x \in A_2} \frac{s^2}{\pi |x - c|^2} < \infty. \tag{1.2.9}$$

Since $A_2$ is a countable set, the right hand side of the above inequality is clearly a convergent series. Combining the above two estimations, we have $D_{s,c}(L) < \infty$, the lemma is proved. □

To give a clearer explanation of (1.2.9), we provide another proof of Lemma 1.2.3. First we prove the following lemma.

**Lemma 1.2.4** *Let $A \in \mathbb{R}^{n\times n}$ be an invertible square matrix of order n, $T = A^T A$ is a positive definite real symmetric matrix. Let $\delta$ be the smallest eigenvalue of $T$, $\delta^*$ is the biggest eigenvalue of $T$, we have $0 < \delta \leqslant \delta^*$, and*

$$\sqrt{\delta} \leqslant |Ax|_{x\in S} \leqslant \sqrt{\delta^*}, \tag{1.2.10}$$

*where $S = \{x \in \mathbb{R}^n \mid |x| = 1\}$ is the unit sphere in $\mathbb{R}^n$.*

***Proof*** Since $T$ is a positive definite real symmetric matrix, so all eigenvalues $\delta_1, \delta_2, \ldots, \delta_n$ of $T$ are positive, and there is an orthogonal matrix $P$ such that

$$P^T T P = \mathrm{diag}\{\delta_1, \delta_2, \ldots, \delta_n\}.$$

Hence,

$$|Ax|^2 = x^T T x = x^T P(P^T T P)P^T x.$$

Since $P^T T P$ is a diagonal matrix, we have

$$\delta |P^T x|^2 \leqslant |Ax|^2 \leqslant \delta^* |P^T x|^2.$$

If $x \in S$, then $|P^T x| = |x| = 1$, so we have $\sqrt{\delta} \leqslant |Ax| \leqslant \sqrt{\delta^*}$. □

By Lemma 1.2.4, and $S$ is a compact set, $|Ax|$ is a continuous function on $S$, so $|Ax|$ can achieve the maximum value on $S$. This maximum value is defined as $||A||$,

$$||A|| = \max\{|Ax| \;\big|\; |x| = 1\}. \tag{1.2.11}$$

We call $\|A\|$ for the matrix norm of $A$, and Lemma 1.2.4 shows that

$$\sqrt{\delta} \leqslant ||A|| \leqslant \sqrt{\delta^*}, \quad \forall A \in GL_n(\mathbb{R}). \tag{1.2.12}$$

**Another proof of Lemma** 1.2.3: Let $L = L(B)$ be any full-rank lattice, $B$ is the generated matrix of $L$. By definition we have

$$D_{s,c}(L) = \sum_{x\in L} D_{s,c}(x) = \frac{1}{s^n} \sum_{x\in L} \mathrm{e}^{-\frac{\pi}{s^2}|x-c|^2} = \frac{1}{s^n} \sum_{x\in \mathbb{Z}^n} \mathrm{e}^{-\frac{\pi}{s^2}|Bx-c|^2}. \tag{1.2.13}$$

From Lemma 1.2.4,

$$\frac{|B^{-1}x|}{|x|} \leqslant ||B^{-1}|| \Rightarrow |B^{-1}x| \leqslant ||B^{-1}||\,|x|,\ \forall x \in \mathbb{R}^n.$$

Let $x = By$, $\delta^*$ is the biggest eigenvalue of $(B^{-1})^T B^{-1}$, we have

$$|y| \leqslant ||B^{-1}||\,|By| \Rightarrow |By| \geqslant \frac{1}{||B^{-1}||}|y| \geqslant |y|/\sqrt{\delta^*},\ \forall y \in \mathbb{R}^n. \tag{1.2.14}$$

The property of the exponential function implies that,

$$\sum_{x\in\mathbb{Z}^n, |Bx-c|>M} \mathrm{e}^{-\frac{\pi}{s^2}|Bx-c|^2} \leqslant \sum_{x\in\mathbb{Z}^n, |Bx-c|\neq 0} \frac{s^{2n}}{\pi^n |Bx-c|^{2n}}. \tag{1.2.15}$$

Since

$$|Bx-c|^{2n} = |B(x-B^{-1}c)|^{2n} \geqslant |x-B^{-1}c|^{2n}/(\delta^*)^n.$$

Denote $x = (x_1, \ldots, x_n)$, $B^{-1}c = (u_1, \ldots, u_n)$, then

$$|x-B^{-1}c|^{2n} = (\sum_{i=1}^{n}(x_i-u_i)^2)^n \geqslant (n\sqrt[n]{\Pi_{i=1}^n (x_i-u_i)^2})^n = n^n \Pi_{i=1}^n (x_i-u_i)^2.$$

By (1.2.15),

$$\sum_{x\in\mathbb{Z}^n, |Bx-c|\neq 0} \frac{s^{2n}}{\pi^n |Bx-c|^{2n}} \leqslant \sum_{x\in\mathbb{Z}^n, |Bx-c|\neq 0} \frac{s^{2n}(\delta^*)^n}{\pi^n n^n} \cdot \frac{1}{\Pi_{i=1}^n (x_i-u_i)^2}$$

$$= \frac{s^{2n}(\delta^*)^n}{\pi^n n^n} \sum_{x_1\in\mathbb{Z}} \frac{1}{(x_1-u_1)^2} \sum_{x_2\in\mathbb{Z}} \frac{1}{(x_2-u_2)^2} \cdots \sum_{x_n\in\mathbb{Z}} \frac{1}{(x_n-u_n)^2},$$

every infinite series on the right hand side of the above equation converges, hence, $D_{s,c}(L) < \infty$. □

By Lemma 1.2.3, we define the discrete Gauss density function $D_{L,s,c}(x)$ as

$$D_{L,s,c}(x) = \frac{D_{s,c}(x)}{D_{s,c}(L)} = \frac{\rho_{s,c}(x)}{\rho_{s,c}(L)}. \tag{1.2.16}$$

Trivially, we have

$$\sum_{x\in L} D_{L,s,c}(x) = 1.$$

So $D_{L,s,c}(x)$ corresponds to a random variable from Gauss distribution defined on the lattice $L$ (discrete geometry) with parameters $s$ and $c$.

**Definition 1.2.4** Let $L = L(B) \subset \mathbb{R}^n$ be a lattice with full rank, $s > 0$ is a given positive real number, $c \in \mathbb{R}^n$ is a given vector, define the discrete Gauss measure function $g_{L,s,c}(x)$ as a function defined on the basic neighborhood $F(B)$ of $L$,

$$g_{L,s,c}(x) = D_{s,c}(\bar{x}) = \frac{1}{s^n} \sum_{y \in L} \rho_{s,c}(x + y), \ x \in F(B). \tag{1.2.17}$$

By Definition and (1.2.3), it is clear that

$$\int_{F(B)} g_{L,s,c}(x)\mathrm{d}x = \frac{1}{s^n} \sum_{y \in L} \int_{F(B)} \rho_{s,c}(x + y)\mathrm{d}x = \frac{1}{s^n} \int_{\mathbb{R}^n} \rho_{s,c}(x)\mathrm{d}x = 1. \tag{1.2.18}$$

Thus, the density function $g_{L,s,c}(x)$ defined on the basic neighborhood $F(B)$ corresponds to a continuous random variable on $F(B)$, denoted as $D_{s,c}\mathrm{mod}L$.

**Lemma 1.2.5** *The random variable $D_{s,c}modL$ is actually defined in the additive quotient group $\mathbb{R}^n/L$.*

***Proof*** $F(B)$ is a set of representative elements of the additive quotient group $\mathbb{R}^n/L$, and we only prove that for any set of representative elements of $\mathbb{R}^n/L$, the discrete Gauss function $g_{L,s,c}(x)$ remains constant, then $D_{s,c} \bmod L$ can be regarded as a random variable on the additive quotient group $\mathbb{R}^n/L$. Actually, if $x_1, x_2 \in \mathbb{R}^n$, $x_1 \equiv x_2 \pmod{L}$, we have $g_{L,s,c}(x_1) = g_{L,s,c}(x_2)$. To obtain the result, by definition

$$g_{L,s,c}(x_1) = D_{s,c}(\bar{x_1}) = \frac{1}{s^n} \sum_{y \in L} \rho_{s,c}(x_1 + y).$$

Since $x_1 = x_2 + y_0$, where $y_0 \in L$, so

$$g_{L,s,c}(x_1) = \frac{1}{s^n} \sum_{y \in L} \rho_{s,c}(x_1 + y) = \frac{1}{s^n} \sum_{y \in L} \rho_{s,c}(x_2 + y_0 + y)$$

$$= \frac{1}{s^n} \sum_{y \in L} \rho_{s,c}(x_2 + y) = D_{s,c}(\bar{x_2}) = g_{L,s,c}(x_2).$$

By $x_1 \equiv x_2 \pmod{L}$, then $\bar{x_1} = \bar{x_2}$ are the same additive cosets in the quotient group $\mathbb{R}^n/L$. Thus, the discrete Gauss measure $g_{L,s,c}(x)$ can be defined on any basic neighborhood of $L$, and the corresponding random variable $D_{s,c} \bmod L$ is actually defined on the quotient group $\mathbb{R}^n/L$. □

## 1.3 Smoothing Parameter

For a given full-rank lattice $L \subset \mathbb{R}^n$, in the previous section we defined the discrete Gauss measure $g_{L,s,c}(x)$, and the corresponding continuous random variable $D_{s,c}$ mod $L$ on the basic neighborhood $F(B)$ of $L$. In this section, we discuss an important parameter on Gauss lattice—the smoothing parameter. The concept of smooth parameters was introduced by Micciancio and Regev in 2007 Micciancio and Regev (2004). For a given vector $x \in \mathbb{R}^n$, we have the following lemma.

**Lemma 1.3.1** *For a given lattice $L \subset \mathbb{R}^n$, we have*

$$\lim_{s\to\infty} \sum_{x\in L} \rho_{1/s}(x) = 1$$

*or equally*

$$\lim_{s\to\infty} \sum_{x\in L\setminus\{0\}} \rho_{1/s}(x) = 0.$$

***Proof*** By the property of the exponential function, when $|x| > M_0$ ($M_0$ is a positive constant) then

$$\mathrm{e}^{-\pi s^2|x|^2} \leqslant \frac{1}{\pi s^2|x|^2}.$$

So

$$\sum_{x\in L} \rho_{1/s}(x) = \sum_{x\in L} \mathrm{e}^{-\pi s^2|x|^2} \leqslant \sum_{|x|\leqslant M_0, x\in L} \mathrm{e}^{-\pi s^2|x|^2} + \frac{1}{\pi s^2} \sum_{|x|>M_0, x\in L} \frac{1}{|x|^2}.$$

The first part of the equation above only has a finite number of terms, so

$$\lim_{s\to\infty} \sum_{|x|\leqslant M_0, x\in L} \mathrm{e}^{-\pi s^2|x|^2} = 1.$$

The second part of the above equation is a convergent series, therefore,

$$\lim_{s\to\infty} \frac{1}{\pi s^2} \sum_{|x|>M_0, x\in L} \frac{1}{|x|^2} = 0.$$

Here, we get the proof. □

By Definition 1.2.3, we have $\rho_{1/s}(L) = \sum_{x\in L} \rho_{1/s}(x)$, then $\rho_{1/s}(L)$ is a monotone decreasing function of $s$. When $s \to \infty$, $\rho_{1/s}(L)$ monotonically decreasing to 1. So we give the definition of smoothing parameter.

**Definition 1.3.1** Let $L \subset \mathbb{R}^n$ be a lattice with full rank, $L^*$ is the dual lattice of $L$, define the smoothing parameter $\eta_\epsilon(L)$ of $L$: For any $\epsilon > 0$, define

$$\eta_\epsilon(L) = \min\{s \mid s > 0,\ \rho_{1/s}(L^*) < 1 + \epsilon\}. \tag{1.3.1}$$

Equally,

$$\eta_\epsilon(L) = \min\{s \mid s > 0,\ \rho_{1/s}(L^* \backslash \{0\}) < \epsilon\}. \tag{1.3.2}$$

By definition, the smoothing parameter $\eta_\epsilon(L)$ of $L$ is a monotone decreasing function of $\epsilon$, namely

$$\eta_{\epsilon_1}(L) \leqslant \eta_{\epsilon_2}(L), \quad \text{if } 0 < \epsilon_2 < \epsilon_1.$$

**Definition 1.3.2** Let $A \subset \mathbb{R}^n$ be a finite or countable set, $X$ and $Y$ are two discrete random variables on $A$, the statistical distance between $X$ and $Y$ is defined as

$$\Delta(X, Y) = \frac{1}{2} \sum_{a \in A} |Pr\{X = a\} - Pr\{Y = a\}|. \tag{1.3.3}$$

If $A$ is a continuous region in $\mathbb{R}^n$, $X$ and $Y$ are continuous random variables on $A$, $T_1(x)$ and $T_2(x)$ are the density functions of $X$ and $Y$, respectively, then the statistical distance between $X$ and $Y$ is defined as

$$\Delta(X, Y) = \frac{1}{2} \int_A |T_1(x) - T_2(x)| \mathrm{d}x. \tag{1.3.4}$$

It can be proved that for any function $f$ defined on $A$, we have

$$\Delta(f(X), f(Y)) \leqslant \Delta(X, Y).$$

From (1.2.17) in the last section, $D_{s,c}$ mod $L$ is a continuous random variable defined on the basic neighborhood $F(B)$ of the lattice $L$ with the density function $g_{L,s,c}(x)$. Let $U(F(B))$ be a uniform random variable defined on $F(B)$ with the density function $d(x) = \frac{1}{\det(L)}$. The main result of this section is that the statistical distance between $D_{s,c}$ mod $L$ and the uniform distribution $U(F(B))$ can be arbitrarily small.

**Theorem 1.1** *For any $s > 0$, given a lattice with full rank $L = L(B) \subset \mathbb{R}^n$, $L^*$ is the dual lattice of $L$, then the statistical distance between the discrete Gauss distribution and the uniform distribution on the basic neighborhood $F(B)$ satisfies*

$$\Delta(D_{s,c} \bmod L, U(F(B))) \leqslant \frac{1}{2} \rho_{1/s}(L^* \backslash \{0\}). \tag{1.3.5}$$

*Particularly, for any $\epsilon > 0$, and any $s \geqslant \eta_\epsilon(L)$, we have*

$$\Delta(D_{s,c} \bmod L, U(F(B))) \leqslant \frac{1}{2}\epsilon. \tag{1.3.6}$$

*To prove Theorem 1.1, we first introduce the following lemma.*

**Lemma 1.3.2** *Suppose $f(x) \in L^1(\mathbb{R}^n)$ and satisfies the following two conditions:*
*(i) $\sum_{x\in L} |f(x+u)|$ uniformly converges in any bounded closed region of $\mathbb{R}^n$ (about $u$);*
*(ii) $\sum_{y\in L^*} |\hat{f}(y)|$ converges. Then*

$$\sum_{x\in L} f(x) = \frac{1}{det(L)} \sum_{y\in L^*} \hat{f}(y),$$

*where $L = L(B) \subset \mathbb{R}^n$ is a full-rank lattice, $L^*$ is the dual lattice, $det(L) = |det(B)|$ is the determinant of the lattice $L$.*

***Proof*** We first consider the case of $B = I_n$, here $L = \mathbb{Z}^n$, $L^* = \mathbb{Z}^n$. By condition (i), let $F(u)$ be

$$F(u) = \sum_{x\in\mathbb{Z}^n} f(x+u), \quad u \in \mathbb{R}^n.$$

Since $F(u)$ is a periodic function of the lattice $\mathbb{Z}^n$, namely $F(u+x) = F(u)$, for $\forall x \in \mathbb{Z}^n$, we have the following Fourier expansion

$$F(u) = \sum_{y\in\mathbb{Z}^n} a(y)\mathrm{e}^{2\pi i u\cdot y}. \tag{1.3.7}$$

Integrating $F(u)\mathrm{e}^{-2\pi i u\cdot x}$ for $u \in [0,1]^n$:

$$\int_{[0,1]^n} F(u)\mathrm{e}^{-2\pi i u\cdot x}\mathrm{d}u = \sum_{y\in\mathbb{Z}^n} \int_{[0,1]^n} a(y)\mathrm{e}^{2\pi i u\cdot(y-x)}\mathrm{d}u = a(x), \ \forall x \in \mathbb{Z}^n.$$

Hence, we have the following Fourier inversion formula:

$$a(y) = \int_{[0,1]^n} F(u)\mathrm{e}^{-2\pi i u\cdot y}\mathrm{d}u = \sum_{x\in\mathbb{Z}^n} \int_{[0,1]^n} f(x+u)\mathrm{e}^{-2\pi i(u+x)\cdot y}\mathrm{d}u$$

$$= \sum_{x\in\mathbb{Z}^n} \int_{x+[0,1]^n} f(z)\mathrm{e}^{-2\pi i z\cdot y}\mathrm{d}z = \int_{\mathbb{R}^n} f(z)\mathrm{e}^{-2\pi i z\cdot y}\mathrm{d}z = \hat{f}(y).$$

From the above equation and (1.3.7),

$$F(u) = \sum_{y\in\mathbb{Z}^n} \hat{f}(y)\mathrm{e}^{2\pi i u\cdot y}.$$

Take $u = 0$, we have

$$F(0) = \sum_{x\in\mathbb{Z}^n} f(x) = \sum_{y\in\mathbb{Z}^n} \hat{f}(y),$$

the lemma is proved for $L = \mathbb{Z}^n$. For the general case $L = L(B)$, since $L^* = L((B^{-1})')$, then

$$\sum_{x\in L} f(x) = \sum_{x\in\mathbb{Z}^n} f(Bx) = \sum_{x\in\mathbb{Z}^n} (f\circ B)(x),$$

where $f\circ B(x) = f(Bx)$. Replace $f(x)$ with $f\circ B$, then $f\circ B$ still satisfies the conditions of this lemma, so

$$\sum_{x\in\mathbb{Z}^n} f\circ B(x) = \sum_{y\in\mathbb{Z}^n} \widehat{f\circ B}(y).$$

From the definition of Fourier transform,

$$\widehat{f\circ B}(y) = \int_{\mathbb{R}^n} f(Bt)\mathrm{e}^{-2\pi i y\cdot t}\mathrm{d}t.$$

Take variable substitution $t = B^{-1}x$, then

$$\begin{aligned}\widehat{f\circ B}(y) &= \frac{1}{|\det(B)|}\int_{\mathbb{R}^n} f(x)\mathrm{e}^{-2\pi i y\cdot B^{-1}x}\mathrm{d}x\\ &= \frac{1}{|\det(B)|}\int_{\mathbb{R}^n} f(x)\mathrm{e}^{-2\pi i (B^{-1})' y\cdot x}\mathrm{d}x\\ &= \frac{1}{|\det(B)|}\hat{f}((B^{-1})'y).\end{aligned}$$

Above all,

$$\sum_{x\in L} f(x) = \sum_{y\in\mathbb{Z}^n} \widehat{f\circ B}(y) = \frac{1}{|\det(B)|}\sum_{y\in\mathbb{Z}^n} \hat{f}((B^{-1})'y) = \frac{1}{|\det(B)|}\sum_{y\in L^*} \hat{f}(y).$$

We finish the proof of this lemma. □

**The proof of Theorem** 1.1 The density function of the continuous random variable $D_{s,c}$ mod $L$ defined on the basic neighborhood $F(B)$ of $L$ is $g_{L,s,c}(x)$, from Eq. (1.2.17) and Lemma 1.3.2, we have

$$g_{L,s,c}(x) = \frac{1}{s^n}\sum_{y\in L}\rho_{s,c}(x+y) = \frac{1}{s^n}\sum_{y\in L}\rho_{s,c-x}(y).$$

By (1.2.5), the Fourier transform of $\rho_{s,c-x}(y)$ is

$$\hat{\rho}_{s,c-x}(y) = \mathrm{e}^{-2\pi i y\cdot(c-x)}s^n\rho_{1/s}(y).$$

Combining with Lemma 1.3.2, we obtain

$$g_{L,s,c}(x) = \frac{1}{|\det(B)|}\sum_{y\in L^*}\mathrm{e}^{2\pi i y\cdot(x-c)}\rho_{1/s}(y). \tag{1.3.8}$$

The density function of the uniformly distributed random variable $U(F(B))$ on $F(B)$ is $\frac{1}{|\det(B)|}$, based on the definition of statistical distance,

$$\begin{aligned}\Delta(D_{s,c} \bmod L, U(F(B))) &= \frac{1}{2}\int_{F(B)}|g_{L,s,c}(x) - \frac{1}{|\det(B)|}|\mathrm{d}x\\ &= \frac{1}{2}\int_{F(B)}|\frac{1}{|\det(B)|}\sum_{y\in L^*,y\neq 0}\mathrm{e}^{2\pi i y\cdot(x-c)}\rho_{1/s}(y)|\mathrm{d}x\\ &\leqslant \frac{1}{2}\mathrm{Vol}(F(B))\det(L^*)\max_{x\in F(B)}|\sum_{y\in L^*\setminus\{0\}}\mathrm{e}^{2\pi i y\cdot(x-c)}\rho_{1/s}(y)|\\ &\leqslant \frac{1}{2}\sum_{y\in L^*\setminus\{0\}}\rho_{1/s}(y) = \frac{1}{2}\rho_{1/s}(L^*\setminus\{0\}).\end{aligned}$$

So (1.3.5) in Theorem 1.1 is proved. From the definition of smoothing parameter $\eta_\epsilon(L)$, when $s \geqslant \eta_\epsilon(L)$, we have

$$\rho_{1/s}(L^*\setminus\{0\}) < \epsilon.$$

Therefore, if $s \geqslant \eta_\epsilon(L)$, we have

$$\Delta(D_{s,c} \bmod L, U(F(B))) \leqslant \frac{1}{2}\epsilon.$$

Thus, Theorem 1.1 is proved. □

Another application of Lemma 1.3.2 is to prove the following inequality.

**Lemma 1.3.3** *Let $a \geqslant 1$ be a given positive real number, then*

$$\sum_{x\in L} e^{-\frac{\pi}{a}|x|^2} \leqslant a^{\frac{n}{2}} \sum_{x\in L} e^{-\pi|x|^2}. \tag{1.3.9}$$

***Proof*** By Definition 1.2.1, the left hand side of the sum in the above inequality can be written as

$$\rho_{\sqrt{a}}(x) = \mathrm{e}^{-\frac{\pi}{a}|x|^2},\ s = \sqrt{a}.$$

Since $\rho_s(x)$ satisfies the conditions of Lemma 1.3.2, we have

$$\sum_{x\in L} \rho_s(x) = \det(L^*) \sum_{x\in L^*} \hat{\rho}_s(x) = \det(L^*) \sum_{x\in L^*} s^n \rho_{1/s}(x).$$

Obviously $\rho_s(x)$ is a monotone increasing function of $s$, take $s = \sqrt{a} \geqslant 1$, then

$$\sum_{x\in L} \rho_{\sqrt{a}}(x) = a^{\frac{n}{2}} \det(L^*) \sum_{x\in L^*} \rho_{\frac{1}{\sqrt{a}}}(x) \leqslant a^{\frac{n}{2}} \det(L^*) \sum_{x\in L^*} \rho(x)$$

$$= a^{\frac{n}{2}} \sum_{x\in L} \rho(x) = a^{\frac{n}{2}} \sum_{x\in L} \mathrm{e}^{-\pi|x|^2}.$$

We complete the proof of Lemma 1.3.3. □

Let $N = N(0, 1)$ be the unit sphere in $\mathbb{R}^n$, namely

$$N = \{x \in \mathbb{R}^n \mid |x| \leqslant 1\}.$$

**Lemma 1.3.4** *Suppose $L \subset \mathbb{R}^n$ is a lattice with full rank, $c > \frac{1}{\sqrt{2\pi}}$ is a positive real number, $C = c\sqrt{2\pi e} \cdot e^{-\pi c^2}$, $v \in \mathbb{R}^n$, then*

$$\rho(L\backslash c\sqrt{n}N) < C^n \rho(L),\ \textit{and}\ \rho((L+v)\backslash c\sqrt{n}N) < 2C^n \rho(L).$$

*That is,*

$$\sum_{x\in L, x\notin c\sqrt{n}N} e^{-\pi|x|^2} < C^n \sum_{x\in L} e^{-\pi|x|^2}, \tag{1.3.10}$$

$$\sum_{x\in L+v, x\notin c\sqrt{n}N} e^{-\pi|x|^2} < 2C^n \sum_{x\in L} e^{-\pi|x|^2}.$$

***Proof*** We will prove the first inequality, ler $t$ be a positive real number, $0 < t < 1$, then

$$\begin{aligned}\sum_{x\in L} \mathrm{e}^{-\pi t|x|^2} &= \sum_{x\in L} \mathrm{e}^{\pi(1-t)|x|^2}\cdot \mathrm{e}^{-\pi|x|^2} \\ &> \sum_{x\in L,|x|^2\geqslant c^2 n} \mathrm{e}^{\pi(1-t)|x|^2}\cdot \mathrm{e}^{-\pi|x|^2} \\ &\geqslant \mathrm{e}^{\pi(1-t)c^2 n} \sum_{x\in L,|x|^2\geqslant c^2 n} \mathrm{e}^{-\pi|x|^2}.\end{aligned}$$

In Lemma 1.3.3, take $a = \frac{1}{t}$, then $a > 1$, we get

$$\sum_{x\in L} \mathrm{e}^{-\pi t|x|^2} \leqslant t^{-\frac{n}{2}} \sum_{x\in L} \mathrm{e}^{-\pi|x|^2}.$$

Hence,

$$\sum_{x\in L,|x|^2\geqslant c^2 n} \mathrm{e}^{-\pi|x|^2} < \mathrm{e}^{-\pi(1-t)c^2 n} \sum_{x\in L} \mathrm{e}^{-\pi t|x|^2} \leqslant \mathrm{e}^{-\pi(1-t)c^2 n} t^{-\frac{n}{2}} \sum_{x\in L} \mathrm{e}^{-\pi|x|^2}.$$

It implies that

$$\rho(L\backslash c\sqrt{n}N) < (t^{-\frac{1}{2}}\mathrm{e}^{-\pi(1-t)c^2})^n \rho(L).$$

Let $t = \frac{1}{2\pi c^2}$, then

$$\rho(L\backslash c\sqrt{n}N) < (c\cdot\sqrt{2\pi e}\cdot \mathrm{e}^{-\pi c^2})^n \rho(L),$$

The second inequality can be proved in the same way. Lemma 1.3.4 holds. □

Based on the above inequality, we can give an upper bound estimation of the smoothing parameter on lattice, which is a very important result about the smoothing parameter.

**Theorem 1.2** *For any $n$ dimensional full-rank lattice $L \subset \mathbb{R}^n$, we have*

$$\eta_{2^{-n}}(L) \leqslant \sqrt{n}/\lambda_1(L^*). \tag{1.3.11}$$

*where $\lambda_1(L^*)$ is the minimal distance of the dual lattice $L^*$ (see (1.0.4)).*

***Proof*** Take $c = 1$ in Lemma 1.3.4, we first prove

$$C = \sqrt{2\pi e}\cdot \mathrm{e}^{-\pi} < \frac{1}{4}. \tag{1.3.12}$$

If we take the logarithm of both sides, then

$$\log(32\pi) + 1 < 2\pi.$$

Since we have the following inequality,

$$\log(32\pi) + 1 < \log 128 + 1 < 2\pi.$$

So (1.3.12) holds. By Lemma 1.3.4, we have

$$\rho(L^*\backslash\sqrt{n}N) < C^n\rho(L^*) = C^n(\rho(L^*\backslash\sqrt{n}N) + \rho(L^* \cap \sqrt{n}N)).$$

From the both sides, we get

$$\rho(L^*\backslash\sqrt{n}N) < \frac{C^n}{1 - C^n}\rho(L^* \cap \sqrt{n}N).$$

If $s > \sqrt{n}/\lambda_1(L^*)$, for all $x \in L^*\backslash\{0\}$,

$$|sx| \geqslant s \cdot \lambda_1(L^*) > \sqrt{n} \Rightarrow sL^* \cap \sqrt{n}N = \{0\}.$$

Hence,

$$\begin{aligned}\rho_{1/s}(L^*) = \rho(sL^*) &= 1 + \rho(sL^*\backslash\sqrt{n}N) \\ &< 1 + \frac{C^n}{1 - C^n}\rho(sL^* \cap \sqrt{n}N) \\ &= 1 + \frac{C^n}{1 - C^n} < 1 + \frac{2^{-2n}}{2^{-n}} = 2^{-n} + 1.\end{aligned}$$

Take $\epsilon = 2^{-n}$, then

$$\eta_{2^{-n}}(L) \leqslant \sqrt{n}/\lambda_1(L^*).$$

Theorem 1.2 is obtained. □

According to the proof of Theorem 1.2, we can further improve the upper bound estimation of the smoothing parameter.

**Corollary 1.3.1** *Let*

$$r = \sqrt{\frac{1}{2\pi} + \frac{\log 2\pi}{2\pi} + \frac{1}{n\pi}\log(1 + 2^n)}. \quad (< 0.82) \tag{1.3.13}$$

*Then for any full-rank lattice $L \subset \mathbb{R}^n$, we obtain*

$$\eta_{2^{-n}}(L) \leqslant r\sqrt{n}/\lambda_1(L^*). \tag{1.3.14}$$

***Proof*** Take $c > r$ in Lemma 1.3.4, then $c > \frac{1}{\sqrt{2\pi}}$, and

$$C = c \cdot \sqrt{2\pi e} \cdot \mathrm{e}^{-\pi c^2} \Rightarrow \frac{C^n}{1 - C^n} < \frac{1}{2^n}. \tag{1.3.15}$$

By Lemma 1.3.4, for any full-rank lattice $L \subset \mathbb{R}^n$, we have

$$\rho(L^* \backslash c\sqrt{n}N) < \frac{C^n}{1 - C^n}\rho(L^* \cap c\sqrt{n}N).$$

If $s > c\sqrt{n}/\lambda_1(L^*)$, for any $x \in L^* \backslash \{0\}$,

$$|sx| \geqslant s\lambda_1(L^*) > c\sqrt{n}.$$

Hence,

$$sL^* \cap c\sqrt{n}N = \{0\}.$$

Therefore,

$$\rho_{1/s}(L^*) = \rho(sL^*) = 1 + \rho(L^* \backslash c\sqrt{n}N) < 1 + \frac{C^n}{1 - C^n} < 1 + \frac{1}{2^n}.$$

Finally we have (let $c \to r$)

$$\eta_{2^{-n}}(L) \leqslant r\sqrt{n}/\lambda_1(L^*).$$

Corollary 1.3.1 is proved. □

**Corollary 1.3.2** *For any $n$ dimensional full-rank lattice $L \subset \mathbb{R}^n$, we have*

$$\eta_{2^{-n}}(L) \leqslant \frac{4}{5}\sqrt{n}/\lambda_1(L^*). \tag{1.3.16}$$

***Proof*** Take $c = \frac{4}{5}$ in Lemma 1.3.4, then $c > \frac{1}{\sqrt{2\pi}}$, and

$$C = c \cdot \sqrt{2\pi e} \cdot \mathrm{e}^{-\pi c^2} \Rightarrow \frac{C^n}{1 - C^n} < \frac{1}{2^n}.$$

Lemma 1.3.4 implies that for any full-rank lattice $L \subset \mathbb{R}^n$, we have

$$\rho(L^* \backslash c\sqrt{n}N) < \frac{C^n}{1 - C^n}\rho(L^* \cap c\sqrt{n}N).$$

If $s > c\sqrt{n}/\lambda_1(L^*)$, for any $x \in L^*\backslash\{0\}$,

$$|sx| \geqslant s\lambda_1(L^*) > c\sqrt{n}.$$

Hence,

$$sL^* \cap c\sqrt{n}N = \{0\}.$$

We get

$$\rho_{1/s}(L^*) = \rho(sL^*) = 1 + \rho(L^*\backslash c\sqrt{n}N) < 1 + \frac{C^n}{1 - C^n} < 1 + \frac{1}{2^n},$$

which implies that

$$\eta_{2^{-n}}(L) \leqslant \frac{4}{5}\sqrt{n}/\lambda_1(L^*).$$

Corollary 1.3.2 is proved. □

In the following, we give another classical upper bound estimation for the smoothing parameter. For any $n$ dimensional full-rank lattice $L \subset \mathbb{R}^n$, we have introduced the definition of minimal distance $\lambda_1(L)$ on lattice, which can actually be generalized to the general case. For $1 \leqslant i \leqslant n$,

$$\lambda_i(L) = \min\{r \mid \dim(L \cap rN(0, 1)) \geqslant i\}. \tag{1.3.17}$$

$\lambda_i(L)$ is also called the $i$-th continuous minimal distance of lattice $L$. To give an upper bound estimation of the smoothing parameter, we first prove the following lemma.

**Lemma 1.3.5** *For any n dimensional full-rank lattice L, $s > 0$, $c \in \mathbb{R}^n$, then*

$$\rho_{s,c}(L) \leqslant \rho_s(L). \tag{1.3.18}$$

***Proof*** According to Lemma 1.3.2, we have

$$\begin{aligned}
\rho_{s,c}(L) &= \det(L^*)\hat{\rho}_{s,c}(L^*) \\
&= \det(L^*) \sum_{y \in L^*} \hat{\rho}_{s,c}(y) \\
&= \det(L^*) \sum_{y \in L^*} \mathrm{e}^{-2\pi i c \cdot y} \hat{\rho}_s(y) \\
&\leqslant \det(L^*) \sum_{y \in L^*} \hat{\rho}_s(y) = \rho_s(L),
\end{aligned}$$

where we have used $\hat{\rho}_{s,c}(y) = \mathrm{e}^{-2\pi i c\cdot y}\hat{\rho}_s(y)$, the lemma gets proved. □

**Theorem 1.3** *For any n dimensional full-rank lattice $L$, $\epsilon > 0$, we have*

$$\eta_\epsilon(L) \leqslant \sqrt{\frac{\ln(2n(1+1/\epsilon))}{\pi}}\lambda_n(L), \tag{1.3.19}$$

*where $\lambda_n(L)$ is the $N$-th continuous minimal distance of the lattice $L$ defined by (1.3.17).*

***Proof*** Let

$$s = \sqrt{\frac{\ln(2n(1+1/\epsilon))}{\pi}}\lambda_n(L),$$

we need to prove $\rho_{1/s}(L^*\backslash\{0\}) \leqslant \epsilon$. From the definition of $\lambda_n(L)$, there are $n$ linearly independent vectors $v_1, v_2, \ldots, v_n$ in $L$ satisfying $|v_i| \leqslant \lambda_n(L)$, and for any positive integer $k > 1$, we have $v_i/k \notin L$, $1 \leqslant i \leqslant n$. The main idea of the proof is to take a segregation of $L^*$, for any integer $j$, let

$$S_{i,j} = \{x \in L^* \mid x \cdot v_i = j\} \subset L^*,$$

for any $y \in L^*\backslash\{0\}$, there is $v_i$ that satisfies $y \cdot v_i \neq 0$ (otherwise we have $y = 0$), which implies $y \notin S_{i,0}$, i.e. $y \in L^*\backslash S_{i,0}$, so we have

$$L^*\backslash\{0\} = \cup_i^n (L^*\backslash S_{i,0}). \tag{1.3.20}$$

To estimate $\rho_{1/s}(L^*\backslash S_{i,0})$, we need some preparations. Let $u_i = v_i/|v_i|^2$, then $|u_i| = 1/|v_i| \geqslant 1/\lambda_n(L)$. $\forall j \in \mathbb{Z}$, $\forall x \in S_{i,j}$,

$$(x - ju_i)\cdot ju_i = jx\cdot u_i - j^2 u_i\cdot u_i = \frac{j^2}{|v_i|^2} - \frac{j^2}{|v_i|^2} = 0.$$

Therefore,

$$|x|^2 = |x - ju_i|^2 + |ju_i|^2.$$

So

$$\rho_{1/s}(S_{i,j}) = \sum_{x\in S_{i,j}} \mathrm{e}^{-\pi s^2|x|^2}$$

$$= \mathrm{e}^{-\pi s^2|ju_i|^2} \sum_{x\in S_{i,j}} \mathrm{e}^{-\pi s^2|x-ju_i|^2}$$

$$= \mathrm{e}^{-\pi s^2|ju_i|^2}\rho_{1/s}(S_{i,j} - ju_i). \tag{1.3.21}$$

Since the inner product of any vector in $S_{i,j} - ju_i$ with $v_i$ is 0, then $S_{i,j} - ju_i$ is actually a translation of $S_{i,0}$, namely there is a vector $w$ satisfying $S_{i,j} - ju_i =$

$S_{i,0} - w$. In fact, for any $x_j \in S_{i,j}, x_0 \in S_{i,0}, w = x_0 - x_j + ju_i$ satisfies the equality $S_{i,j} - ju_i = S_{i,0} - w$. By Lemma 1.3.5, we have

$$\rho_{1/s}(S_{i,j} - ju_i) = \rho_{1/s}(S_{i,0} - w) = \rho_{1/s,w}(S_{i,0}) \leqslant \rho_{1/s}(S_{i,0}). \tag{1.3.22}$$

Combine (1.3.21) with (1.3.22),

$$\rho_{1/s}(S_{i,j}) \leqslant \mathrm{e}^{-\pi s^2 |ju_i|^2} \rho_{1/s}(S_{i,0}) \leqslant \mathrm{e}^{-\pi (s/\lambda_n(L))^2 j^2} \rho_{1/s}(S_{i,0}).$$

When $x > 1$, it follows that

$$\sum_{j \neq 0} x^{-j^2} \leqslant 2 \sum_{j>0} x^{-j} = \frac{2}{x-1}.$$

Next, we will estimate $\rho_{1/s}(L^* \backslash S_{i,0})$,

$$\begin{aligned}
\rho_{1/s}(L^* \backslash S_{i,0}) &= \sum_{j \neq 0} \rho_{1/s}(S_{i,j}) \\
&\leqslant \sum_{j \neq 0} \mathrm{e}^{-\pi (s/\lambda_n(L))^2 j^2} \rho_{1/s}(S_{i,0}) \\
&\leqslant \frac{2}{\mathrm{e}^{\pi (s/\lambda_n(L))^2} - 1} \rho_{1/s}(S_{i,0}) \\
&= \frac{2}{\mathrm{e}^{\pi (s/\lambda_n(L))^2} - 1} (\rho_{1/s}(L^*) - \rho_{1/s}(L^* \backslash S_{i,0})).
\end{aligned}$$

So we get

$$\rho_{1/s}(L^* \backslash S_{i,0}) \leqslant \frac{2}{\mathrm{e}^{\pi (s/\lambda_n(L))^2} + 1} \rho_{1/s}(L^*).$$

From (1.3.20),

$$\rho_{1/s}(L^* \backslash \{0\}) \leqslant \sum_{i=1}^{n} \rho_{1/s}(L^* \backslash S_{i,0}) \leqslant \frac{2n}{\mathrm{e}^{\pi (s/\lambda_n(L))^2} + 1} \rho_{1/s}(L^*).$$

Together with $\rho_{1/s}(L^*) = 1 + \rho_{1/s}(L^* \backslash \{0\})$, we have

$$\rho_{1/s}(L^* \backslash \{0\}) \leqslant \frac{2n}{\mathrm{e}^{\pi (s/\lambda_n(L))^2} + 1 - 2n} < \frac{2n}{\mathrm{e}^{\pi (s/\lambda_n(L))^2} - 2n} = \epsilon.$$

In the last equality, we have used that

$$s = \sqrt{\frac{\ln(2n(1+1/\epsilon))}{\pi}}\lambda_n(L).$$

Based on the definition of the smoothing parameter,

$$\eta_\epsilon(L) \leqslant \sqrt{\frac{\ln(2n(1+1/\epsilon))}{\pi}}\lambda_n(L).$$

Theorem 1.3 is proved. □

At the end of this section, we present an inequality for the minimal distance on lattice, which will be used in the next chapter when we prove that the LWE problem is polynomial equivalent with the hard problems on lattice.

**Lemma 1.3.6** *For any n dimensional lattice L, $\epsilon > 0$, we have*

$$\eta_\epsilon(L) \geqslant \sqrt{\frac{\ln 1/\epsilon}{\pi}}\frac{1}{\lambda_1(L^*)} \geqslant \sqrt{\frac{\ln 1/\epsilon}{\pi}}\frac{\lambda_n(L)}{n}. \tag{1.3.23}$$

***Proof*** Let $v \in L^*$ and $|v| = \lambda_1(L^*)$, $s = \eta_\epsilon(L)$, from the definition of smoothing parameter, we have

$$\epsilon = \rho_{1/s}(L^*\backslash\{0\}) \geqslant \rho_{1/s}(v) = \mathrm{e}^{-\pi s^2\lambda_1^2(L^*)}.$$

Hence,

$$s \geqslant \sqrt{\frac{\ln 1/\epsilon}{\pi}}\frac{1}{\lambda_1(L^*)}.$$

That is, the first inequality in this lemma holds. For the second inequality, Theorem 2.1 in Banaszczyk (1993) implies that

$$1 \leqslant \lambda_1(L^*)\lambda_n(L) \leqslant n, \tag{1.3.24}$$

so we immediately get the second inequality. The lemma holds. □

## 1.4 Some Properties of Discrete Gauss Distribution

In this section we introduce some properties about the discrete Gauss distribution. First we give the definition of the expectation of discrete Gauss distribution.

**Definition 1.4.1** Let $m, n$ be two positive integers, $L \subset \mathbb{R}^n$ be an $n$ dimensional full-rank lattice, $c \in \mathbb{R}^n, s > 0, \xi$ is a random variable from the discrete Gauss distribution $D_{L,s,c}$, and $f : \mathbb{R}^n \to \mathbb{R}^m$ is a given function, we denote

$$E[\xi] = \sum_{\xi = x \in L} x D_{L,s,c}(x) \tag{1.4.1}$$

as the expectation of $\xi$, and denote

$$E[f(\xi)] = \sum_{\xi = x \in L} f(x) D_{L,s,c}(x) \tag{1.4.2}$$

as the expectation of $f(\xi)$.

**Lemma 1.4.1** *For any n dimensional full-rank lattice, $L \subset \mathbb{R}^n$, $c, u \in \mathbb{R}^n$, $|u| = 1$, $0 < \epsilon < 1$, $s \geqslant 2\eta_\epsilon(L)$, $\xi$ is a random variable from the discrete Gauss distribution $D_{L,s,c}$, then we have*

$$|E[(\xi - c) \cdot u]| \leqslant \frac{\epsilon s}{1 - \epsilon}, \tag{1.4.3}$$

*and*

$$|E[((\xi - c) \cdot u)^2] - \frac{s^2}{2\pi}| \leqslant \frac{\epsilon s^2}{1 - \epsilon}. \tag{1.4.4}$$

***Proof*** Let $L' = L/s = \{\frac{x}{s} \mid x \in L\}$, $c' = c/s$, $\xi'$ is a random variable from the discrete Gauss distribution $D_{L',c'}$, for any $x \in L'$, we have

$$Pr\{\xi' = x\} = \frac{\rho_{c'}(x)}{\rho_{c'}(L')} = \frac{\rho_{s,c}(sx)}{\rho_{s,c}(L)} = Pr\{\xi = sx\}.$$

That is, $Pr\{\frac{\xi}{s} = x\} = Pr\{\xi' = x\}, \forall x \in L'$, therefore,

$$E[(\xi - c) \cdot u] = sE[(\frac{\xi}{s} - c') \cdot u] = sE[(\xi' - c') \cdot u],$$

the inequality (1.4.3) is equivalent to

$$|E[(\xi' - c') \cdot u]| \leqslant \frac{\epsilon}{1 - \epsilon}. \tag{1.4.5}$$

Similarly, the inequality (1.4.4) is equivalent to

$$|E[((\xi' - c') \cdot u)^2] - \frac{1}{2\pi}| \leqslant \frac{\epsilon}{1 - \epsilon}. \tag{1.4.6}$$

So we only need to prove the two inequalities for $s = 1$. Denote $\xi$ as a random variable from the discrete Gauss distribution $D_{L,c}$, the condition $s \geqslant 2\eta_\epsilon(L)$ in Lemma 1.4.1

becomes $\eta_\epsilon(L) \leqslant \frac{1}{2}$. We prove that the two inequalities (1.4.5) and (1.4.6) hold if $u = (1, 0, \ldots, 0)$ firstly. For any positive integer $j$, let

$$g_j(x) = (x_1 - c_1)^j \rho_c(x),$$

where $x = (x_1, x_2, \ldots, x_n)$, $c = (c_1, c_2, \ldots, c_n)$. Let $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$, then

$$E[((\xi - c) \cdot u)^j] = E[(\xi_1 - c_1)^j] = \frac{g_j(L)}{\rho_c(L)}.$$

Based on Lemma 1.3.2,

$$E[((\xi - c) \cdot u)^j] = \frac{g_j(L)}{\rho_c(L)} = \frac{\det(L^*)\hat{g}_j(L^*)}{\det(L^*)\hat{\rho}_c(L^*)} = \frac{\hat{g}_j(L^*)}{\hat{\rho}_c(L^*)}. \tag{1.4.7}$$

In order to estimate $\hat{\rho}_c(L^*)$, from Lemma 1.2.1 we get $\hat{\rho}_c(x) = \mathrm{e}^{-2\pi i x \cdot c}\rho(x)$, thus, $|\hat{\rho}_c(x)| = \rho(x)$, note that $\eta_\epsilon(L) \leqslant \frac{1}{2} < 1$,

$$|\hat{\rho}_c(L^*)| = |1 + \sum_{x \in L^* \setminus \{0\}} \hat{\rho}_c(x)| \geqslant 1 - \sum_{x \in L^* \setminus \{0\}} |\hat{\rho}_c(x)| = 1 - \rho(L^* \setminus \{0\}) \geqslant 1 - \epsilon. \tag{1.4.8}$$

To estimate $\hat{g}_j(L^*)$, assume $\rho_c^{(j)}(x)$ is the $j$ order partial derivative of $\rho_c(x)$ about the first variable $x_1$, i.e.

$$\rho_c^{(j)}(x) = (\frac{\partial}{\partial x_1})^j \rho_c(x).$$

If $j = 1, 2$, it is easy to get

$$\rho_c^{(1)}(x) = -2\pi(x_1 - c_1)\rho_c(x).$$

$$\rho_c^{(2)}(x) = (4\pi^2(x_1 - c_1)^2 - 2\pi)\rho_c(x).$$

It follows that

$$g_1(x) = -\frac{1}{2\pi}\rho_c^{(1)}(x).$$

$$g_2(x) = \frac{1}{4\pi^2}\rho_c^{(2)}(x) + \frac{1}{2\pi}\rho_c(x).$$

Since $\widehat{\rho_c^{(j)}}(x) = (2\pi i x_1)^j \hat{\rho}_c(x)$, we have

$$\hat{g}_1(x) = -i x_1 \hat{\rho}_c(x).$$

$$\hat{g}_2(x) = (\frac{1}{2\pi} - x_1^2)\hat{\rho}_c(x).$$

According to the inequality $|x_1| \leqslant \sqrt{|x|^2} \leqslant \mathrm{e}^{\frac{|x|^2}{2}}$ and $\eta_\epsilon(L) \leqslant \frac{1}{2}$,

$$|\hat{g}_1(L^*)| \leqslant \sum_{x\in L^*} |x_1| \cdot |\hat{\rho}_c(x)| = \sum_{x\in L^*\backslash\{0\}} |x_1|\rho(x) \leqslant \sum_{x\in L^*\backslash\{0\}} \mathrm{e}^{\frac{|x|^2}{2}} \mathrm{e}^{-\pi|x|^2}$$

$$\leqslant \sum_{x\in L^*\backslash\{0\}} \mathrm{e}^{-\frac{\pi}{4}|x|^2} = \rho_2(L^*\backslash\{0\}) \leqslant \epsilon. \tag{1.4.9}$$

Combining (1.4.7), (1.4.8) and (1.4.9) together,

$$|E[(\xi - c)\cdot u]| = \frac{|\hat{g}_1(L^*)|}{|\hat{\rho}_c(L^*)|} \leqslant \frac{\epsilon}{1-\epsilon}.$$

For a general unit vector $u \in \mathbb{R}^n$, there exists an orthogonal matrix $M \in \mathbb{R}^{n\times n}$ such that $Mu = (1, 0, \ldots, 0)$. Denote $\eta$ as a random variable from the discrete Gauss distribution $D_{M^{-1}L, M^{-1}c}$, for any $x \in L$,

$$Pr\{\eta = M^{-1}x\} = \frac{\rho_{M^{-1}c}(M^{-1}x)}{\rho_{M^{-1}c}(M^{-1}L)} = \frac{\mathrm{e}^{-\pi|M^{-1}x - M^{-1}c|^2}}{\rho_{M^{-1}c}(M^{-1}L)}$$

$$= \frac{\mathrm{e}^{-\pi|x-c|^2}}{\rho_c(L)} = Pr\{\xi = x\} = Pr\{M^{-1}\xi = M^{-1}x\},$$

which implies that the distributions of $\eta$ and $M^{-1}\xi$ are the same, hence,

$$|E[(\xi - c)\cdot u]| = |E[M^{-1}(\xi - c)\cdot Mu]| = |E[(\eta - M^{-1}c)\cdot Mu]| \leqslant \frac{\epsilon}{1-\epsilon}.$$

Above all the inequality (1.4.3) holds, and inequality (1.4.4) could be proved in the same way. We complete the proof of Lemma 1.4.1. □

**Lemma 1.4.2** *For any $n$ dimensional full-rank lattice $L \subset \mathbb{R}^n$, $c \in \mathbb{R}^n$, $0 < \epsilon < 1$, $s \geqslant 2\eta_\epsilon(L)$, $\xi$ is a random variable from the discrete Gauss distribution $D_{L,s,c}$, then we have*

$$|E[\xi - c]|^2 \leqslant (\frac{\epsilon}{1-\epsilon})^2 s^2 n, \tag{1.4.10}$$

*and*

$$E[|\xi - c|^2] \leqslant (\frac{1}{2\pi} + \frac{\epsilon}{1-\epsilon}) s^2 n. \tag{1.4.11}$$

***Proof*** Let $u_1, u_2, \ldots, u_n$ be the $n$ unit column vectors of $n \times n$ matrix $I_n$, by Lemma 1.4.1,

$$|E[\xi - c]|^2 = \sum_{i=1}^{n} (E[(\xi - c)\cdot u_i])^2 \leqslant (\frac{\epsilon}{1-\epsilon})^2 s^2 n.$$

$$E[|\xi - c|^2] = \sum_{i=1}^{n} E[((\xi - c) \cdot u_i)^2] \leqslant (\frac{1}{2\pi} + \frac{\epsilon}{1-\epsilon})s^2 n.$$

Lemma 1.4.2 holds. □

**Lemma 1.4.3** *For any n dimensional full-rank lattice $L \subset \mathbb{R}^n$, $v \in \mathbb{R}^n$, $0 < \epsilon < 1$, $s \geqslant \eta_\epsilon(L)$, $\xi$ is a random variable from the discrete Gauss distribution $D_{L,s,v}$, then we have*

$$Pr\{|\xi - v| > s\sqrt{n}\} \leqslant \frac{1+\epsilon}{1-\epsilon} 2^{-n}. \tag{1.4.12}$$

***Proof*** From the proof of Lemma 1.4.1, here we only need to prove for the case $s = 1$. Since

$$Pr\{|\xi - v| > \sqrt{n}\} = \sum_{x \in L, |x-v| > \sqrt{n}} \frac{\rho_v(x)}{\rho_v(L)}$$

$$= \sum_{x \in L, |x-v| > \sqrt{n}} \frac{\rho(x-v)}{\rho_v(L)} = \frac{\rho((L-v)\backslash \sqrt{n}N)}{\rho_v(L)},$$

take $c = 1$ in Lemma 1.3.4 and get

$$\rho((L-v)\backslash \sqrt{n}N) < 2^{-n}\rho(L).$$

That is,

$$Pr\{|\xi - v| > \sqrt{n}\} < 2^{-n} \frac{\rho(L)}{\rho_v(L)}. \tag{1.4.13}$$

Based on Lemma 1.3.2, Lemma 1.2.1 and $\eta_\epsilon(L) \leqslant 1$,

$$\rho_v(L) = |\rho_v(L)| = |\det(L^*)\hat{\rho}_v(L^*)| = |\det(L^*) \sum_{x \in L^*} \mathrm{e}^{-2\pi i x \cdot v} \rho(x)|$$

$$\geqslant |\det(L^*)|(1 - \sum_{x \in L^* \backslash \{0\}} |\mathrm{e}^{-2\pi i x \cdot v} \rho(x)|) = |\det(L^*)|(1 - \sum_{x \in L^* \backslash \{0\}} \rho(x))$$

$$= |\det(L^*)|(1 - \rho(L^* \backslash \{0\})) \geqslant |\det(L^*)|(1-\epsilon). \tag{1.4.14}$$

Similarly,

$$\rho(L) = |\rho(L)| = |\det(L^*)\hat{\rho}(L^*)|$$

$$= |\det(L^*) \sum_{x \in L^*} \rho(x)| = |\det(L^*)|(1 + \sum_{x \in L^* \backslash \{0\}} \rho(x))$$

$$= |\det(L^*)|(1 + \rho(L^* \backslash \{0\})) \leqslant |\det(L^*)|(1+\epsilon). \tag{1.4.15}$$

Combining (1.4.13), (1.4.14) and (1.4.15) together, it follows that

$$Pr\{|\xi - v| > \sqrt{n}\} \leqslant \frac{1+\epsilon}{1-\epsilon} 2^{-n}.$$

This lemma holds. □

For $x \in \mathbb{R}^n$ and a set $A \subset \mathbb{R}^n$, we define the distance from $x$ to $A$ as $\text{dist}(x, A) = \min_{y \in A} |x - y|$.

**Lemma 1.4.4** *For any n dimensional full-rank lattice $L \subset \mathbb{R}^n$, $c, v \in \mathbb{R}^n$, $0 < \epsilon < 1$, $s \geqslant \eta_\epsilon(L)$, $\xi$ is a random variable from the discrete Gauss distribution $D_{L,s,c}$, $dist(v, L^*) \geqslant \frac{\sqrt{n}}{s}$, then*

$$|E[e^{2\pi i \xi \cdot v}]| \leqslant \frac{1+\epsilon}{1-\epsilon} 2^{-n}. \tag{1.4.16}$$

***Proof*** From the proof of Lemma 1.4.1, we only need to prove for the case $s = 1$. Let

$$g(x) = \mathrm{e}^{2\pi i x \cdot v} \rho_c(x).$$

By Lemma 1.3.2,

$$E[\mathrm{e}^{2\pi i \xi \cdot v}] = \frac{g(L)}{\rho_c(L)} = \frac{\det(L^*)\hat{g}(L^*)}{\det(L^*)\hat{\rho}_c(L^*)} = \frac{\hat{g}(L^*)}{\hat{\rho}_c(L^*)}.$$

We have proved that $|\hat{\rho}_c(L^*)| \geqslant 1 - \epsilon$ in Lemma 1.4.1, based on (iii) of Lemma 1.1.2 and Lemma 1.2.1,

$$\hat{g}(x) = \hat{\rho}_c(x - v) = \rho(x - v)\mathrm{e}^{-2\pi i (x-v)\cdot c},$$

therefore,

$$|\hat{g}(L^*)| = |\sum_{x \in L^*} \rho(x - v)\mathrm{e}^{-2\pi i (x-v)\cdot c}| \leqslant \sum_{x \in L^*} \rho(x - v) = \rho(L^* - v).$$

Since $\text{dist}(v, L^*) \geqslant \sqrt{n}$, we know

$$\rho(L^* - v) = \rho((L^* - v) \backslash \sqrt{n} N).$$

Take $c = 1$ in Lemma 1.3.4 and get

$$\rho((L^* - v) \backslash \sqrt{n} N) < 2^{-n} \rho(L^*) = 2^{-n}(1 + \rho(L^* \backslash \{0\})) \leqslant 2^{-n}(1 + \epsilon).$$

Above all,

$$|E[\mathrm{e}^{2\pi i \xi \cdot v}]| = |\frac{\hat{g}(L^*)}{\hat{\rho}_c(L^*)}| \leqslant \frac{1+\epsilon}{1-\epsilon} 2^{-n}.$$

We complete the proof of Lemma 1.4.4. □

**Lemma 1.4.5** *For any $n$ dimensional full-rank lattice $L \subset \mathbb{R}^n$, $w, c, v \in \mathbb{R}^n$, $0 < \epsilon < 1$, $s \geqslant \eta_\epsilon(L)$, $\xi$ is a random variable from the discrete Gauss distribution $D_{L,s,c}$, $dist(v, L^*) \geqslant \frac{\sqrt{n}}{s}$, then*

$$|E[\cos(2\pi(\xi + w) \cdot v)]| \leqslant \frac{1+\epsilon}{1-\epsilon} 2^{-n}. \tag{1.4.17}$$

***Proof*** By Lemma 1.4.4 we have

$$|E[\cos(2\pi(\xi + w) \cdot v)]| \leqslant |E[e^{2\pi i(\xi+w)\cdot v}]| = |E[e^{2\pi i \xi \cdot v}]| \leqslant \frac{1+\epsilon}{1-\epsilon} 2^{-n}.$$

Lemma 1.4.5 holds. □

Finally, we give a lemma which will be used in the next chapter.

**Lemma 1.4.6** *Let $v_1, v_2, \ldots, v_m$ be $m$ independent random variables on $\mathbb{R}^n$ such that $E[|v_i|^2] \leqslant l$ and $|E[v_i]|^2 \leqslant \epsilon$ for $i = 1, 2, \ldots, m$. Then for any $z = (z_1, z_2, \ldots, z_m)^T \in \mathbb{R}^m$,*

$$E[|\sum_{i=1}^{m} z_i v_i|^2] \leqslant (l + m\epsilon)|z|^2. \tag{1.4.18}$$

***Proof*** By Cauchy inequality we get $\sum_{i=1}^{m} |z_i| \leqslant \sqrt{m}|z|$, so

$$E[|\sum_{i=1}^{m} z_i v_i|^2] = \sum_{i,j} z_i z_j E[v_i \cdot v_j] = \sum_i z_i^2 E[|v_i|^2] + \sum_{i \neq j} z_i z_j E[v_i] \cdot E[v_j]. \tag{1.4.19}$$

The first term of the right hand side in (1.4.19) has the estimation

$$\sum_i z_i^2 E[|v_i|^2] \leqslant \sum_i z_i^2 l = l|z|^2.$$

The second term of the right hand side in (1.4.19) has the estimation

$$\sum_{i \neq j} z_i z_j E[v_i] \cdot E[v_j] \leqslant \sum_{i \neq j} |z_i||z_j| \cdot \frac{1}{2}(|E[v_i]|^2 + |E[v_j]|^2)$$

$$\leqslant \sum_{i \neq j} \epsilon |z_i||z_j| \leqslant \epsilon(\sum_i |z_i|)^2 \leqslant m\epsilon|z|^2.$$

From (1.4.19) it follows that

$$E[|\sum_{i=1}^{m} z_i v_i|^2] \leqslant (l + m\epsilon)|z|^2.$$

This lemma holds. □



# Chapter 2
# Reduction Principle of Ajtai


In 1996, the famous scholar Ajtai proposed the reduction principle from the worst case to the average case at the 28th Summer Symposium of the American Computer Society (ACM), named the Ajtai reduction principle [see Ajtai (1996), Ajtai (1999) and Ajtai and Dwork (1997)]. Subsequently, Ajtai and Dwork presented the first lattice-based cryptosystem, which is called the Ajtai-Dwork cryptosystem in the academic circles. The proof of this cryptosystem resisting Shor's quantum computing is to apply Ajtai reduction principle to transform searching for collision points of the Hash function into the SIS problem, and Ajtai reduction principle proves that the difficulty of solving the SIS problem is polynomially equivalent to the shortest vector problem on lattice. The main purpose of this chapter is to prove the Ajtai reduction principle.

## 2.1 Random Linear System

Let $A \in \mathbb{Z}_q^{n\times m}$ be an $n \times m$ matrix on $\mathbb{Z}_q$, if each element of $A$ is a random variable on $\mathbb{Z}_q$, and the $n \times m$ random variables are independent and identically distributed, then $A$ is called a random matrix on $\mathbb{Z}_q$. We give the definition of random linear system

$$y \equiv Ax + z \pmod q,\ x \in \mathbb{Z}_q^m,\ y \in \mathbb{Z}_q^n,\ z \in \mathbb{Z}_q^n, \tag{2.1.1}$$

where $x, y, z$ are random variables on $\mathbb{Z}_q^m$ and $\mathbb{Z}_q^n$, respectively. This random linear system plays an important role in modern cryptography. We prove some basic properties in this section.

**Lemma 2.1.1** *Let $A \in \mathbb{Z}_q^{n\times n}$ be an invertible square matrix of order $n$, $y \equiv Ax \pmod q$, then $y$ is uniformly at random on $\mathbb{Z}_q^n$ if and only if $x$ is uniformly distributed.*



Z. Zheng et al., *Modern Cryptography Volume 2*, Financial Mathematics and Fintech,
https://doi.org/10.1007/978-981-19-7644-5_2

***Proof*** If $x$ is uniformly distributed on $\mathbb{Z}_q^n$, then for any $x_0 \in \mathbb{Z}_q^n$, we have

$$Pr\{x = x_0\} = \frac{1}{q^n}.$$

Since there is only one $y_0 \in \mathbb{Z}_q^n \Rightarrow Ax_0 \equiv y_0 \pmod{q}$, therefore,

$$Pr\{y = y_0\} = Pr\{x = x_0\} = \frac{1}{q^n}.$$

Because $A$ is an invertible matrix, there is a one-to-one correspondence between $y_0$ and $x_0$. In other words, when $x_0$ traverses all the vectors in $\mathbb{Z}_q^n$, $y_0$ also traverses all the vectors in $\mathbb{Z}_q^n$, which means $y$ is also uniformly at random on $\mathbb{Z}_q^n$. On the other hand, if $y$ is uniformly distributed on $\mathbb{Z}_q^n$, so is $x$ on $\mathbb{Z}_q^n$ by $x \equiv A^{-1}y \pmod{q}$. □

***Remark 2.1.1*** In fact, for the above linear system, $x$ and $y$ are random variables with the same distribution when $A$ is an invertible square matrix. However, this property doesn't hold if $A$ is not a square matrix.

Let $a \in \mathbb{R}$ be a real number, $[a]$ be the greatest integer no more than $a$, i.e. $[a]$ is the only integer satisfying the following inequality,

$$[a] \leqslant a < [a] + 1.$$

If $x \in \mathbb{R}^n$ is an $n$ dimensional vector, $x = (x_1, x_2, \ldots, x_n)$, we define $[x]$ as follows

$$[x] = ([x_1], [x_2], \ldots, [x_n]) \in \mathbb{Z}^n.$$

$[x]$ is called the integer vector of $x$. We say $x$ is a random vector, which means each element $x_j$ is a random variable, and the $n$ random variables are mutually independent.

**Lemma 2.1.2** *If $x \in [0, 1)^n$ is a continuous random variable uniformly distributed on the unit cube, then $[qx]$ is a discrete random variable uniformly on $\mathbb{Z}_q^n$.*

***Proof*** Since all the components of $x$ are independent, we only prove for $n = 1$. If $a \in [0, 1)$ is a continuous random variable uniformly distributed, then for any $i = 0, 1, \ldots, q-1$, we have

$$Pr\{[qa] = i\} = Pr\{i \leqslant qa < i + 1\} = Pr\{\frac{i}{q} \leqslant a < \frac{i+1}{q}\} = \frac{1}{q}.$$

This indicates $[qa]$ is a discrete random variable uniformly distributed on $\mathbb{Z}_q$. □

**Lemma 2.1.3** *Let $L = L(B)$ be a n dimensional full-rank lattice, $F(B)$ is the basic neighbourhood of $L$. If $x$ is a random variable uniformly distributed on $F(B)$, then $[qB^{-1}x]$ is a discrete random variable uniformly on $\mathbb{Z}_q^n$.*

***Proof*** $\forall a \in \mathbb{Z}_q^n$, we have

$$Pr\{[qB^{-1}x] = a\} = Pr\{\frac{Ba}{q} \leqslant x < \frac{B(a+1)}{q}\}.$$

Since the volume of basic neighbourhood $F(B)$ is $\det(L) = |\det(B)|$, the probability density function of $x$ is $\frac{1}{\det(L)}$, thus,

$$Pr\{\frac{Ba}{q} \leqslant x < \frac{B(a+1)}{q}\} = \int_{\frac{Ba}{q}}^{\frac{B(a+1)}{q}} \frac{1}{\det(L)} \mathrm{d}y = \int_{\frac{a}{q}}^{\frac{a+1}{q}} \frac{|\det(B)|}{\det(L)} \mathrm{d}u = \frac{1}{q^n}.$$

We set $y = Bu$ in the above equality, and get

$$Pr\{[qB^{-1}x] = a\} = \frac{1}{q^n}.$$

So $[qB^{-1}x]$ is uniformly distributed on $\mathbb{Z}_q^n$. □

## 2.2 SIS Problem

The SIS problem plays a very important role in modern lattice cryptography, which is to find the shortest nonzero integer solution in a class of random linear systems.

**Definition 2.2.1** Let $n, m, q$ be positive integers, $m \geqslant n$, $A \in \mathbb{Z}_q^{n \times m}$ is a uniformly distributed random matrix on $\mathbb{Z}_q$, $\beta \in \mathbb{R}$, $0 < \beta < q$. The SIS problem is to find the shortest nonzero integer vector $z \in \mathbb{Z}^m$ such that

$$Az \equiv 0 \ (\mathrm{mod}\ q), \ \text{and } z \neq 0, \ |z| \leqslant \beta. \tag{2.2.1}$$

We call the above SIS problem with parameters $n, m, q, A, \beta$ as $\mathrm{SIS}_{n,q,\beta,m}$, and $A$ is called as the coefficient matrix of SIS problem.

***Remark 2.2.1*** If $m < n$, since the number of variables is less than equations, (2.2.1) is not guaranteed to have a nonzero solution, so we suppose that $m \geqslant n$. If $\beta \geqslant q$, let

$z = \begin{pmatrix} q \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{Z}^m$, we have $Az \equiv 0 \pmod{q}$, and $|z| = q < \beta$. This solution is trivial so that we always assume that $\beta < q$ in Definition 2.2.1.

***Remark 2.2.2*** The difficulty of SIS problem decreases when $m$ becomes larger, while it increases as $n$ becomes larger. In fact, if $z$ is a solution of $\mathrm{SIS}_{n,q,\beta,m}$, $m' > m$, $[A, A']$ is the coefficient matrix of $\mathrm{SIS}_{n,q,\beta,m'}$. Let $z' = \begin{pmatrix} z \\ 0 \end{pmatrix}$, then

$$[A, A']z' = [Az, 0] \equiv 0 \pmod{q}.$$

So $z'$ is a solution of $\mathrm{SIS}_{n,q,\beta,m'}$. If a solution satisfies $n+1$ equations of SIS problem, it also satisfies $n$ equations of SIS problem. Therefore, the difficulty of SIS problem increases when $n$ becomes larger.

**Lemma 2.2.1** *For any positive integer $q$, any $A \in \mathbb{Z}_q^{n\times m}$, and $\beta \geqslant \sqrt{m}q^{\frac{n}{m}}$, the SIS problem has a nonzero solution; i.e. there exists a vector $z \in \mathbb{Z}^m$, $z \neq 0$, such that*

$$Az \equiv 0 \ (mod\ q), \ \ and\ |z| \leqslant \beta.$$

***Proof*** Let $z = \begin{pmatrix} z_1 \\ \vdots \\ z_m \end{pmatrix} \in \mathbb{Z}^m$, we consider the value of coordinate $z_i$ in $0 \leqslant z_i \leqslant q^{\frac{n}{m}}$. It's easy to check that there are more than $q^n$ such integer vectors. Thus, we can find $z'$ and $z''$ such that $z' \neq z''$, $Az' \equiv Az'' \pmod{q}$, i.e.

$$A(z' - z'') \equiv 0 \pmod{q}, \ \text{and}\ |z' - z''| \leqslant \sqrt{m}q^{\frac{n}{m}} \leqslant \beta.$$

We complete the proof. □

By the above Lemma and Remark 2.2.1, in order to guarantee there is a non-trivial solution of the SIS problem, we always assume the following conditions of parameters

$$n < m, \ \sqrt{m}q^{\frac{n}{m}} \leqslant \beta < q. \tag{2.2.2}$$

Since the difficulty of SIS problem decreases when $\beta$ becomes larger, we always suppose that

$$\beta = \sqrt{m}q^{\frac{n}{m}}. \tag{2.2.3}$$

Furthermore, we call $n$ as the security parameter of SIS problem, $m = m(n), q = q(n), \beta = \beta(n)$ are functions of $n$. By (2.2.2) and (2.2.3), if $m$ and $q$ are polynomial

functions of $n$ written as $m = \text{poly}(n)$, $q = \text{poly}(n)$, then $\beta$ is also a polynomial function of $n$, i.e. $\beta = \text{poly}(n)$. Let $U(\mathbb{Z}_q^{n\times m})$ be all the $n \times m$ random matrices uniformly distributed on $\mathbb{Z}_q$, we call all the possible SIS problems as $\text{SIS}_{q,m}$, i.e.

$$\text{SIS}_{q,m} = \{q(n), U(\mathbb{Z}_q^{n\times m}), \beta(n)\}_n.$$

$\text{SIS}_{q,m}$ problem is called the total SIS problem, which plays an 'average case' role in the Ajtai reduction principle. The parameters are selected as

$$m = \text{poly}(n),\ q = \text{poly}(n),\ q^{\frac{n}{m(n)}} = O(1) \Rightarrow \beta = O(\sqrt{m}). \tag{2.2.4}$$

**Definition 2.2.2** Let $A \in U(\mathbb{Z}_q^{n\times m})$, $\text{SIS'}_{n,q,\beta,m}$ problem is to find $z \in \mathbb{Z}^n$, $z \notin 2\mathbb{Z}^n$, such that

$$Az \equiv 0 \ (\text{mod}\ q),\ \text{and}\ |z| \leqslant \beta.$$

In fact the goal of SIS' problem is to find a solution of SIS problem with at least one odd integer of all the coordinates. The relation between solutions of the two problems could be summarized in the following lemma.

**Lemma 2.2.2** *Suppose $q$ is an odd integer, then there is a polynomial time algorithm from the solution of SIS problem to SIS' problem.*

***Proof*** If $z = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \in \mathbb{Z}^n$ is a solution of SIS problem, then there exists an integer $k \geqslant 0$, such that $2^{-k}z \notin 2\mathbb{Z}^n$. Let $z' = 2^{-k}z$, since $q$ is an odd integer, based on $Az \equiv 0 \ (\text{mod}\ q)$, we have

$$Az' = 2^{-k}Az \equiv 0 \ (\text{mod}\ q),$$

and $|z'| = 2^{-k}|z| \leqslant 2^{-k}\beta$. This means $z'$ is a solution of SIS' problem. The complexity of calculating $z'$ from $z$ is polynomial (polynomial function of $n$), and this is because

$$\text{Time}\{\text{compute } z'\} = O(n\log^2 q) = \text{poly}(n).$$

The above formula also holds even if $q$ is an exponential function of $n$. □

SIS problem and Ajtai-Dwork cryptosystem have close relation. Let $f_A(z) = Az$ be Hash function, $z'$ and $z''$ be the collision points of $f_A(z)$, then

$$f_A(z') \equiv f_A(z'') \ (\text{mod}\ q) \Rightarrow A(z' - z'') \equiv 0 \ (\text{mod}\ q).$$

It's easy to obtain a solution of SIS problem if we can find two collision points of $f_A$. In this sense, Hash function $f_A(z)$ is strongly collision resisted. The security of Ajtai-Dwork cryptosystem mainly depends on the difficulty of solving SIS problem.

SIS problem could be regarded as the shortest vector problem in the average case. Let

$$\Lambda_q^{\perp}(A) = \{z \in \mathbb{Z}^m \mid Az \equiv 0 \pmod{q}\}.$$

Then $\Lambda_q^{\perp}(A)$ is an $m$ dimensional $q$-ary integer lattice. In fact, solving SIS problem is equivalent to find the shortest vector of $\Lambda_q^{\perp}(A)$.

If $A \in U(\mathbb{Z}_q^{n\times m})$ is the coefficient matrix of SIS problem, we can discuss SIS problem by transforming it to Hermite form. Let rank$A = n$, the matrix $A_1 \in \mathbb{Z}_q^{n\times n}$ constructed by the first $n$ column vectors of $A$ is an invertible matrix. Suppose $A = [A_1, A_2]$, replace $A$ with $A_1^{-1}A$, we have

$$A_1^{-1}A = [I_n, \bar{A} = A_1^{-1}A_2]. \tag{2.2.5}$$

Since $A_2$ is a random matrix uniformly distributed, by Lemma 2.1.1, $\bar{A}$ is also a uniform random matrix with dimension $n \times (m-n)$.

**Lemma 2.2.3** *The solution set of SIS problem with coefficient matrix $A$ is the same as that of coefficient matrix $A_1^{-1}A$.*

***Proof*** Let $z \in \mathbb{Z}^m$ such that

$$Az \equiv 0 \pmod{q}, \text{ and } 0 < |z| \leqslant \beta.$$

Then $A_1^{-1}Az \equiv 0 \pmod{q}$, $z$ is the solution of SIS problem with coefficient matrix $A_1^{-1}A$. On the other hand, if $A_1^{-1}Az \equiv 0 \pmod{q} \Rightarrow Az \equiv 0 \pmod{q}$, Lemma 2.2.3 holds. □

We call the coefficient matrix $A_1^{-1}A$ determined by (2.2.5) as the normal form of SIS problem.

Finally, we define some hard problems on lattice. We always suppose $L = L(B) \subset \mathbb{R}^n$ is a full-rank lattice, $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the lengths of the continuous shortest vectors in lattice $L$, $\lambda_1$ is the length of shortest vector in $L$, $\gamma = \gamma(n) \geqslant 1$ is a positive function of $n$.

**Definition 2.2.3** (1) SVP$_\gamma$: find a nonzero vector $x$ in lattice $L$ such that

$$|x| \leqslant \gamma(n)\lambda_1(L). \tag{2.2.6}$$

(2) GapSVP$_\gamma$: determine the minimal distance $\lambda_1 = \lambda_1(L)$ of lattice $L$,

$$\lambda_1(L) \leqslant 1, \text{ or } \lambda_1(L) > \gamma(n). \tag{2.2.7}$$

(3) SIVP$_\gamma$: find a set of $n$ linearly independent lattice vectors $S = \{s_i\} \subset L$, such that

$$|S| = \max |s_i| \leqslant \gamma(n)\lambda_n(L). \tag{2.2.8}$$

(4) $\mathrm{BDD}_\gamma$: let $d = \lambda_1(L)/2\gamma(n)$ be the decoding distance of lattice $L$. For any target vector $t \in \mathbb{R}^n$, if

$$\mathrm{dis}(t, L) = \min_{x \in L} |x - t| < d = \lambda_1(L)/2\gamma(n), \tag{2.2.9}$$

then there exists only one lattice vector $v \in L \Rightarrow |v - t| < d$. The bounded decoding distance problem $\mathrm{BDD}_\gamma$ is to find the only lattice point $v$.

The above Definition 2.2.3 gives four kinds of hard problems on lattice. $\mathrm{SVP}_\gamma$ is called the approximation problem of the shortest vector. $\mathrm{GapSVP}_\gamma$ is called the determination problem of the shortest vector. $\mathrm{SIVP}_\gamma$ is called the approximation problem of the shortest linearly independent group. $\mathrm{BDD}_\gamma$ is called the approximation problem of bounded decoding distance problem.

Since parameter $\gamma(n) \geqslant 1$, the bounded decoding distance $d$ satisfies

$$d = \lambda_1(L)/2\gamma(n) \leqslant \frac{1}{2}\lambda_1(L).$$

If the target vector $t \in \mathbb{R}^n$ satisfies the above decoding distance, i.e. $\mathrm{dis}(t, L) < d$, it is easy to see there is only one lattice vector $v \in L \Rightarrow |v - t| < d$. In fact, if $v_1 \in L$, $v_2 \in L \Rightarrow |v_1 - t| < d,\ |v_2 - t| < d$, by triangle inequality

$$|v_1 - v_2| \leqslant |v_1 - t| + |v_2 - t| < 2d \leqslant \lambda_1(L).$$

This has a contradiction with that the minimal distance of lattice $L$ is $\lambda_1(L)$.

The Ajtai reduction principle is said that the above $\mathrm{SIVP}_\gamma$ and $\mathrm{GapSVP}_\gamma$ problems are polynomial equivalent with average case SIS problem. We will prove this in the next section.

## 2.3 INCGDD Problem

Let $S = \{\alpha_i\} \subset \mathbb{R}^n$ be a set of vectors in $\mathbb{R}^n$, we define

$$|S| = \max_i |\alpha_i|. \tag{2.3.1}$$

**Definition 2.3.1** Let $L = L(B) \subset \mathbb{R}^n$ be a full-rank lattice, $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subset L$ be a set of any $n$ linearly independent vectors in $L$, $t \in \mathbb{R}^n$ be the target vector, $r > \gamma(n)\phi(B)$ be a real number. INCGDD problem is to find a lattice vector $\alpha \in L$ such that

$$|\alpha - t| \leqslant \frac{1}{g}|S| + r, \tag{2.3.2}$$

where $g, \gamma(n)$ and $\phi(B)$ are parameters. Under the given parameter system, INCGDD problem could be written as $\text{INCGDD}^{\phi}_{\gamma,g}$.

***Remark 2.3.1*** The key of the INCGDD problem is that for the set $S$ of any given $n$ linearly independent vectors and any target vector $t \in \mathbb{R}^n$, to find a lattice point $\alpha \in L$, such that the distance between $\alpha$ and the target vector is no more than $\frac{1}{g}|S| + r$. By the nearest plane algorithm of Babai, for any $S$ and $t$, there exists a polynomial algorithm finding

$$|\alpha - t| \leqslant \frac{1}{2}\sqrt{n}|S|. \tag{2.3.3}$$

In general, the above formula cannot be improved. We can give a counterexample. Let $L = \mathbb{Z}^n$, $S = I_n$ be an identity matrix, the target vector $t = (\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2})$, then $\forall \alpha \in \mathbb{Z}^n$, we have

$$|\alpha - t| \geqslant \sqrt{\frac{n}{4}} = \frac{1}{2}\sqrt{n} = \frac{1}{2}\sqrt{n}|S|.$$

So there is no lattice point $\alpha$ with the distance no more than $\frac{1}{4}|S|$ from $t$.

Based on the above counterexample, the parameter selection for INCGDD problem is generally $g = 4$. $r$ in (2.3.2) is called the controlled remainder, which could guarantee the existence of lattice vector $\alpha$. Under given parameter system, the INCGDD problem can be transformed into the SIS problem of the corresponding parameter system. This transformation is the key idea of Ajtai reduction principle. We call this transformation algorithm the oracle algorithm, written as $\mathcal{A}(B, S, t)$.

**oracle algorithm** $\mathcal{A}(B, B, 0)$.

We first explain how the oracle algorithm works in a very special case. Let $S = B$ be the generated matrix of $L$, the target vector $t = 0$, parameters of corresponding SIS problem are as follows

$$q(n) = n^4,\ m(n) = n\log n,\ \beta(n) = n. \tag{2.3.4}$$

Since $\beta \geqslant \sqrt{m}q^{\frac{n}{m}}$, by Lemma 2.2.1, the total SIS problem $\text{SIS}_{q,m}$ has a solution.

The oracle sampling algorithm that converts the INCGDD problem into the SIS problem is actually a probabilistic algorithm, which can be divided into the following four steps.

The first step: let $F(B)$ be the basic neighbourhood of $L = L(B)$, defined by

$$F(B) = \{Bx \mid x \in [0, 1)^n\}.$$

We select a point $c \in F(B)$ uniformly in $F(B)$. Let $y \in L$ be the nearest lattice vector to $c$, we obtain a pair of vectors $(c, y)$. Repeat this process independently $m$ times and get $m$ pairs of vectors $(c_1, y_1), (c_2, y_2), \ldots, (c_m, y_m)$, here $m > n$.

The second step: for each $c_i$ $(1 \leqslant i \leqslant m)$, we define $\hat{c}_i$,

$$\hat{c}_i = B[qB^{-1}c_i]/q,\ 1 \leqslant i \leqslant m. \tag{2.3.5}$$

Let $c_i = Bx_i$, where $x_i = (x_{i_1}, x_{i_2}, \ldots, x_{i_n})^T \in [0, 1)^n$, so we have

$$\frac{1}{q}[qB^{-1}c_i] = (\frac{1}{q}[qx_{i_1}], \frac{1}{q}[qx_{i_2}], \ldots, \frac{1}{q}[qx_{i_n}]).$$

Each coordinate satisfies

$$0 \leqslant \frac{1}{q}[qx_{i_j}] \leqslant x_{i_j} < 1,\ j = 1, 2, \ldots, n.$$

Thus, $\hat{c}_i \in F(B)$. Let $c_i - \hat{c}_i = Bv_i$, $v_i = (v_{i_1}, v_{i_2}, \ldots, v_{i_n})^T$, then

$$0 \leqslant v_{i_j} = x_{i_j} - \frac{1}{q}[qx_{i_j}] < \frac{1}{q}. \tag{2.3.6}$$

Therefore, the distance between $\hat{c}_i$ and $c_i$ has the following estimation. Suppose $B = [\beta_1, \ldots, \beta_n]$, it follows that

$$|\hat{c}_i - c_i| = |\sum_{k=1}^{n} \beta_k v_{i_k}| \leqslant \sum_{k=1}^{n} |v_{i_k}||\beta_k|$$

$$\leqslant \frac{n}{q}|B| = \frac{1}{n^3}|B|. \text{ (since } q = n^4)$$

The above formula holds for all $1 \leqslant i \leqslant m$. We can give a geometric interpretation of $\hat{c}_i$. Divide the basic neighbourhood $F(B)$ into $q^n$ polyhedra with side length $\frac{1}{q}$, and each polyhedron is denoted as $\triangle_i$, where

$$\triangle_i = \{Bx \mid x = (x_1, x_2, \ldots, x_n)^T,\ \frac{k-1}{q} \leqslant x_k < \frac{k}{q},\ 1 \leqslant k \leqslant q\}.$$

Since $\{c_i\}_{i=1}^m$ are uniformly distributed in $F(B)$, each polyhedron $\triangle_i$ contains at least one $c$ point under positive probability, written as $c_i$. Based on $\text{Vol}(\triangle_i) = \frac{1}{q^n}\det(L)$, so

$$Pr\{c_i \in \triangle_i\} = \frac{1}{q^n} > 0. \tag{2.3.7}$$

According to (2.3.5), both $\hat{c}_i$ and $c_i$ are contained in the polyhedron $\triangle_i$, and $\hat{c}_i$ is the point at the bottom left corner of $\triangle_i$. From Lemma 2.1.3, since $\{c_i\}$ is uniformly at random in $F(B)$, then $\frac{1}{q}[qB^{-1}c_i]$ is uniformly distributed. Based on Lemma 2.1.1, $\{\hat{c}_i\}$ is also uniformly distributed at random. Let

$$\begin{cases} C = [c_1, c_2, \ldots, c_m]_{n\times m}. \\ Y = [y_1, y_2, \ldots, y_m]_{n\times m}. \\ \hat{C} = [\hat{c_1}, \hat{c_2}, \ldots, \hat{c_m}]_{n\times m}. \end{cases} \tag{2.3.8}$$

We get three $n \times m$ matrices.

The third step: now we define $m$ $n$ dimensional vectors $a_i \in \mathbb{Z}_q^n$, $1 \leqslant i \leqslant m$ in $\mathbb{Z}_q$

$$a_i \equiv [qB^{-1}c_i] \pmod{q},\ 1 \leqslant i \leqslant m.$$

Then

$$A = [a_1, a_2, \ldots, a_m]_{n\times m} \in \mathbb{Z}_q^{n\times m}. \tag{2.3.9}$$

According to Lemma 2.1.3, $A$ is a random matrix uniformly distributed. Suppose $z$ is a solution of $\mathrm{SIS}_{q,m,\beta}$ problem, i.e.

$$Az \equiv 0 \pmod{q}, \text{and}\, 0 < |z| \leqslant \beta,\ z \in \mathbb{Z}^m.$$

Combining $z$ and $\{\hat{c_i}\}$,

$$\hat{C}z = [B[qB^{-1}c_1]/q, \ldots, B[qB^{-1}c_m]/q]z = B \cdot \frac{1}{q}Az \in L(B).$$

Since $Az \equiv 0 \pmod{q} \Rightarrow \frac{1}{q}Az \in \mathbb{Z}^n$, we get a lattice vector $\hat{C}z \in L$.

The four step: Similarly, combining $z$ and $\{c_i\}_{i=1}^m$, $\{y_i\}_{i=1}^m$, we get two vectors $Yz$ and $Cz$. Let $z = (z_1, z_2, \ldots, z_m)^T$, then

$$Yz = [y_1, y_2, \ldots, y_m] \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix} = \sum_{i=1}^{m} z_i y_i \in L.$$

Both $\hat{C}z$ and $Yz$ are lattice vectors, let $\alpha = \hat{C}z - Yz = (\hat{C} - Y)z \in L$. We are to prove that $\alpha$ is a solution of INCGDD problem. Denote $|z|_1$ as the $l_1$ norm of $z$, it follows that

$$|z|_1 = \sum_{i=1}^{m} |z_i| \leqslant \sqrt{m}|z|. \tag{2.3.10}$$

The major part of the length of $\alpha = \hat{C}z - Yz$ is $|Cz - \hat{C}z|$, which could be estimated as follows

$$|Cz - \hat{C}z| = |\sum_{i=1}^{m}(c_i - \hat{c_i})z_i| \leqslant \frac{n}{q}|B||z|_1 \leqslant \frac{n\sqrt{m}\beta}{q}|B|. \tag{2.3.11}$$

Select the parameters $m = n\log n$, $q = n^4$, $\beta = n$, when $n$ is sufficiently large we have,

$$|Cz - \hat{C}z| \leqslant \frac{1}{4}|B|.$$

The minor part of length $|Cz - Yz|$ of $\alpha$ could be calculated by the nearest plane algorithm of Babai [see (2.3.3)]:

$$|Cz - Yz| \leqslant \frac{1}{2}\sqrt{n}|B|.$$

Let $\phi(B) = |B|$, $\gamma(n) = \frac{1}{2}\sqrt{n}$, then

$$|\alpha| = |\hat{C}z - Yz| \leqslant |Cz - \hat{C}z| + |Cz - Yz| \leqslant \frac{1}{4}|B| + r,$$

where $r \geqslant \gamma(n)\phi(B)$. In other words, based on a solution $z$ of the $\mathrm{SIS}_{q,m,\beta}$ problem, we can get a solution of the $\mathrm{INCGDD}^{\phi}_{\gamma,g}$ problem for generated matrix $B$ and the target vector $t = 0$ by a probabilistic polynomial oracle algorithm. Here the parameters are chosen as $g = 4$, $\gamma(n) = \frac{1}{2}\sqrt{n}$, $\phi(B) = |B|$.

The above oracle algorithm is a simple simulation of the reduction principle for INCGDD problem by setting $S = B$ and the target vector $t = 0$. Given any $n$ linearly independent vectors $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subset L$ and target vector $t \in \mathbb{R}^n$, general oracle algorithm $\mathcal{A}(B, S, t)$ will complete the whole technical process of transforming the INCGDD problem into the SIS problem, which is the core idea of Ajtai reduction principle. We begin from two lemmas.

**Lemma 2.3.1** (Sampling lemma) *Let $L = L(B) \subset \mathbb{R}^n$ be a full-rank lattice, $F(B)$ be the basic neighbourhood, $t \in \mathbb{R}^n$ be the target vector, $s \geqslant \eta_\epsilon(L)$ be a positive real number. Then there exists a probabilistic polynomial time algorithm $T(B, t, s)$ to find a pair of vectors $(c, y) \in F(B) \times L(B)$ such that*

*(i) The distribution of vector $c \in F(B)$ is within statistical distance $\frac{1}{2}\epsilon$ from the uniform distribution over $F(B)$.*

*(ii) The conditional distribution of $y \in L$ given $c$ is discrete Gauss distribution $D_{L,s,(t+c)}$.*

***Proof*** The process of sampling algorithm $T(B, t, s)$ could be proved as follows:

1. Since the density function of Gauss distribution $D_{s,t}(x)$ is

$$D_{s,t}(x) = \frac{1}{s^n} e^{-\frac{\pi}{s^2}|x-t|^2},$$

the corresponding random variable is denoted as $D_{s,t}$. Let $r \in \mathbb{R}^n$ comes from distribution $D_{s,t}$, and $r$ is called the noise vector.

2. Let $c \in F(B)$, $c \equiv -r \pmod{L}$, $y = c + r \in L$ be output vectors, $(c, y)$ be the output result.

Since $r$ is generated by Gauss distribution in $\mathbb{R}^n$, it follows that $c$ has the distribution $-D_{s,t} \bmod L$ in the basic neighbourhood $F(B)$. We can prove

$$-D_{s,t} \bmod L = D_{s,-t} \bmod L. \tag{2.3.12}$$

Then the statistical distance between the $c$ and the uniform distribution on $F(B)$ is

$$\Delta(c, U(F(B))) = \Delta(-D_{s,t} \bmod L, U(F(B))) = \Delta(D_{s,-t} \bmod L, U(F(B))) \leqslant \frac{1}{2}\epsilon.$$

On the other hand, $y = c + r \in L$, if $c$ is fixed, the distribution of $y \in L$ is the discrete Gauss distribution $D_{L,s,(t+c)}$. We complete the proof. □

**Lemma 2.3.2** (Combining lemma) *Let $q$ be a positive integer, $L = L(B) \subset \mathbb{R}^n$ be a full-rank lattice, $F(B)$ be the basic neighbourhood. For any full-rank subset $L(S) \subset L(B)$, where $S = [\alpha_1, \alpha_2, \ldots, \alpha_n]$, there is a probabilistic polynomial time algorithm $T_1(B, S)$, for $m$ vectors $C = [c_1, c_2, \ldots, c_m]$ uniformly at random in $F(B)$, we can find a random matrix $A \in \mathbb{Z}_q^{n \times m}$ uniformly distributed and a lattice vector $x \in L(B)$, such that*

$$|x - Cz| \leqslant \frac{1}{q} n\sqrt{m}|S||z|, \tag{2.3.13}$$

*where $z \in \mathbb{Z}^m$, and $Az \equiv 0$ (mod $q$).*

***Proof*** Suppose $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subset L$ are $n$ linearly independent lattice vectors, and $S = [\alpha_1, \alpha_2, \ldots, \alpha_n]$ generates the full-rank lattice $L(S) \subset L(B)$. Let $F(S)$ be the basic neighbourhood of lattice $L(S)$. It is easy to see that $F(B) \subset F(S)$. For any $m$ vectors $\{c_i\}_{i=1}^m$ uniformly distributed in $F(B)$, we can choose $m$ lattice vectors $\{v_1, v_2, \ldots, v_m\} \subset L(B)$ by sampling lemma. The corresponding vector in the basic neighbourhood $F(S)$ is denoted as $v_i \bmod L(S)$, such that

$$\{v_i \bmod L(S)\}_{i=1}^m \subset F(S) \text{ are uniformly distributed.}$$

In other words $\{v_i\}$ is selected from the quotient group $L(B)/L(S)$, satisfying $v_i \not\equiv v_j \pmod{L(S)}$, and $\{v_i \bmod L(S)\}_{i=1}^m$ are uniformly distributed in $F(S)$. We still write $v_i \pmod{L(S)}$ as $v_i$, and let

$$w_i = c_i + v_i \bmod L(S),\ i = 1, 2, \ldots, m.$$

It follows that $\{w_i\}$ is uniformly at random in $F(S)$. For $1 \leqslant i \neq j \leqslant m$, we have

$$v_i \not\equiv v_j \pmod{L(S)} \Rightarrow v_i + F(B) \not\equiv v_j + F(B) \pmod{L(S)},$$

so $\{v_i + F(B)\}_{i=1}^m$ forms a split of $F(S)$ with the same volume. We get $\{w_i\} \subset F(S)$ is uniformly distributed according to $\{v_i\}$ is uniformly at random. Suppose the following two matrices $C$ and $W$ are

$$C = [c_1, c_2, \ldots, c_m], \ W = [w_1, w_2, \ldots, w_m]. \tag{2.3.14}$$

Define $m$ vectors uniformly distributed in $\mathbb{Z}_q^n$ as

$$a_i \equiv [qS^{-1}w_i] \ (\text{mod } q), \ i = 1, 2, \ldots, m. \tag{2.3.15}$$

By Lemma 2.1.3, since $\{w_i\}$ is uniformly at random in $F(S)$, then $A = [a_1, a_2, \ldots, a_m]$ is an $n \times m$ dimensional uniform matrix, $A \in \mathbb{Z}_q^{n\times m}$. Let $z \in \wedge_q^{\perp}(A)$, then

$$z \in \mathbb{Z}_q^m, \text{ and } Az \equiv 0 \ (\text{mod } q).$$

Define the vector $x$

$$x = (C - W + \frac{1}{q}SA)z. \tag{2.3.16}$$

We first prove $x \in L(B)$ is a lattice vector. From the definition of vector $x$, we have

$$x = (C - W + \frac{1}{q}SA)z = \sum_{i=1}^{m}(c_i - w_i)z_i + \frac{1}{q}SAz.$$

Note that

$$c_i - w_i = ((c_i + v_i) - w_i) - v_i, \ 1 \leqslant i \leqslant m,$$

since $c_i + v_i \equiv w_i \ (\text{mod } L(S)) \Rightarrow$

$$c_i + v_i - w_i \in L(S) \subset L(B),$$

and each $v_i$ satisfies $v_i \in L$, it follows that $c_i - w_i \in L$, $1 \leqslant i \leqslant m$. On the other hand $\frac{1}{q}Az \in \mathbb{Z}^n$, we get $\frac{1}{q}SAz \in L(S)$. Thus, we confirm that $x \in L$. Finally, we estimate the distance between $x$ and $Cz$.

$$|x - Cz| = |\sum_{i=1}^{m}(w_i - \frac{S}{q}a_i)z_i| = \frac{1}{q}|S\sum_{i=1}^{m}(u_i - [u_i])z_i|, \tag{2.3.17}$$

where $u_i = qS^{-1}w_i$. It is easy to see, for any $d = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} \in \mathbb{R}^n$,

$$|Sd| = |\sum_{i=1}^{n} d_i s_i| \leqslant \sum_{i=1}^{n} |d_i||s_i| \leqslant |S||d|_1. \tag{2.3.18}$$

Since

$$|\sum_{i=1}^{m}(u_i - [u_i])z_i|_1 \leqslant \sum_{i=1}^{m} |z_i||u_i - [u_i]|_1 \leqslant n\sum_{i=1}^{m} |z_i| \leqslant n\sqrt{m}|z|,$$

by (2.3.17) and (2.3.18) we get

$$|x - Cz| \leqslant \frac{1}{q} n\sqrt{m}|S||z|.$$

So we finish the proof. □

## 2.4 Reduction Principle

The Ajtai reduction principle is to solve hard problems on lattice in general case. For example, SVP, SIVP and GapSVP problems can be transformed to SIS problem by a polynomial algorithm with positive probability, so the difficulty of SIS problem is polynomial equivalent with that of lattice problems. This principle from general to average case is called Ajtai reduction principle from the worst case to the average case in academic circles.

We start by proving that the INCGDD problem could be transformed to the SIS problem. Denote the $\text{INCGDD}^{\phi}_{\gamma,g}$ problem with parameters as $\{B, S, t, r\}$. For any $n$ linearly independent vectors $S$ in a full-rank lattice $L = L(B)$ and any target vector $t \in \mathbb{R}^n$, our goal is to solve a lattice vector $s \in L$ such that

$$|s - t| \leqslant \frac{1}{g}|S| + r, \tag{2.4.1}$$

where $g > 0$ is a positive real number, $r > \gamma(n)\phi(B)$.

**Theorem 2.4.1** (From INCGDD to SIS) *Given parameters $g = g(n) > 0$, $m$, $\beta$ are polynomial functions of $n$, i.e. $m = n^{O(1)}$, $\beta = n^{O(1)}$, $\epsilon = \epsilon(n)$ is a negligible function of $n$, i.e. $\epsilon < \frac{1}{n^k}$ $(k > 0)$, $\phi(B) = \eta_\epsilon(L)$, and*

$$\gamma(n) = \beta(n)\sqrt{n},\ q = q(n) \geqslant g(n)n\sqrt{m}\beta(n). \tag{2.4.2}$$

*Under the above parameter system, there is a probabilistic polynomial algorithm, which could transform the $\text{INCGDD}^{\phi}_{\gamma,g}$ problem to the SIS problem.*

***Proof*** The probabilistic polynomial algorithm in Theorem 2.4.1 is called the oracle algorithm, written as $\mathcal{A}(B, S, t)$. In the last section, we introduce the oracle algorithm detailedly in special case with $S = B$ and the target vector $t = 0$. Now we give the work procedure of general oracle algorithm $\mathcal{A}(B, S, t)$ by sampling Lemma 2.3.1 and combining Lemma 2.3.2:

1. Select two integers $j$ and $\alpha$ uniformly at random, such that

$$j \in \{1, 2, \ldots, m\}, \ -\beta \leqslant \alpha \leqslant \beta, \ \alpha \neq 0.$$

For a given target vector $t \in \mathbb{R}^n$, and positive integer $j$, we define $m$ vectors $t_i$ $(1 \leqslant i \leqslant m)$ as

$$t_i = \begin{cases} -\frac{1}{\alpha}t, & \text{if } i = j. \\ 0, & \text{if } i \neq j. \end{cases} \tag{2.4.3}$$

2. For each $i = 1, 2, \ldots, m$, according to the sampling algorithm $T(B, t_i, \frac{2r}{\gamma})$ in Lemma 2.3.1, i.e. let $t = t_i$, $s = \frac{2}{\gamma}r$, we get

$$(c_i, y_i) \in F(B) \times L(B).$$

Note that $r \geqslant \gamma(n)\phi(B)$, so

$$s = \frac{2r}{\gamma} \geqslant 2\phi(B) = 2\eta_\epsilon(L).$$

3. Define two matrices

$$C = [c_1, c_2, \ldots, c_m], \ Y = [y_1, y_2, \ldots, y_m].$$

4. Based on the given matrices $S \subset L(B)$, $C \in F(B)^m$ and the parameter $q$, we can find a uniform random matrix $A \in \mathbb{Z}_q^{n \times m}$, a solution $z$ of the corresponding SIS problem, and a lattice vector $x \in L(B)$ by the combining algorithm in Lemma 2.3.2 satisfying

$$|x - Cz| \leqslant \frac{1}{q}n\sqrt{m}|S||z| \leqslant \frac{|S|}{g}. \tag{2.4.4}$$

5. Let $s = x - Yz$, then $s \in L(B)$ is a solution of the INCGDD problem, such that

$$|s - t| \leqslant \frac{1}{g}|S| + r \tag{2.4.5}$$

holds with a positive probability. The above oracle algorithm $\mathcal{A}(B, S, t)$ could be represented in the following graph

$$t \in \mathbb{R}^n \xrightarrow[\text{Algorithm}]{\text{Sampling}} \begin{bmatrix} t_1 \to (c_1, y_1) \\ \vdots \\ t_m \to (c_m, y_m) \end{bmatrix} \xrightarrow[Y \in L(B)^m]{C \in F(B)^m} \begin{bmatrix} W \in F(S)^m \\ A \in \mathbb{Z}_q^{n \times m} \end{bmatrix} \xrightarrow[\text{Algorithm}]{\text{Combining}} \begin{bmatrix} x \in L(B) \\ z \in \mathbb{Z}_q^m \end{bmatrix} \to s$$

Since $x, Yz \in L(B)$, it follows that $s = x - Yz \in L(B)$. Next we are to estimate the probability that the inequality $|s - t| \leqslant \frac{1}{g}|S| + r$ holds. We write $\delta > 0$ as the positive probability when solving the SIS problem successfully. The event $H_{j,\alpha}$ denotes getting a solution $z = (z_1, z_2, \ldots, z_m)^T$ of the SIS problem with $z_j = \alpha$, and its probability is $\delta_{j,\alpha}$, where $1 \leqslant j \leqslant m$, $-\beta \leqslant \alpha \leqslant \beta$, $\alpha \neq 0$. If we obtain a solution $z$ of the SIS problem successfully, then at least one of these $2m\beta$ events $H_{j,\alpha}$ occurs. Therefore,

$$\sum_{j,\alpha} \delta_{j,\alpha} \geqslant \delta,$$

there is a pair of $j, \alpha$ such that $Pr\{H_{j,\alpha}\} = \delta_{j,\alpha} \geqslant \frac{\delta}{2m\beta} > 0$. We assume that the event $H_{j,\alpha}$ occurs and estimate the conditional probability of $|s - t| \leqslant \frac{1}{g}|S| + r$. Let $T = [t_1, t_2, \ldots, t_m]$, then $Tz = t_j z_j = -t$. By the triangle inequality,

$$|s - t| \leqslant |x - Cz| + |(C - Y)z - t| \leqslant \frac{|S|}{g} + |(Y - C - T)z|.$$

We have

$$Pr\{|s - t| \leqslant \frac{1}{g}|S| + r\} \geqslant Pr\{|(Y - C - T)z| \leqslant r\}.$$

Based on the sampling Lemma 2.3.1, $y_i$ has discrete Gauss distribution $D_{L(B),\frac{2r}{\gamma},c_i+t_i}$. According to Lemma 2.4.2 in Sect. 1.4, it follows that

$$E[|y_i - (c_i + t_i)|^2] \leqslant (\frac{1}{2\pi} + \frac{\epsilon}{1-\epsilon})(\frac{2r}{\gamma})^2 n,$$

and

$$|E[y_i - (c_i + t_i)]|^2 \leqslant (\frac{\epsilon}{1-\epsilon})^2(\frac{2r}{\gamma})^2 n.$$

Since $y_1, y_2, \ldots, y_m$ are independent, by Lemma 4.6 in section 1.4,

$$E[|\sum_{i=1}^{m}(y_i - (c_i + t_i))z_i|^2] \leqslant (\frac{1}{2\pi} + \frac{\epsilon}{1-\epsilon} + m(\frac{\epsilon}{1-\epsilon})^2)(\frac{2r}{\gamma})^2 n|z|^2 \leqslant \frac{1}{6}(\frac{2r}{\gamma})^2 n|z|^2.$$

Combining $|z| \leqslant \beta$ and $\gamma = \beta\sqrt{n}$, we get

$$E[|(Y - C - T)z|^2] \leqslant \frac{1}{6}(\frac{2r}{\gamma})^2 n|z|^2 \leqslant \frac{2}{3}r^2.$$

Using Chebyshev inequality,

$$Pr\{|(Y - C - T)z| > r\} \leqslant \frac{1}{r^2} E[|(Y - C - T)z|^2] \leqslant \frac{2}{3}.$$

By (4.6),

$$Pr\{|s - t| \leqslant \frac{1}{g}|S| + r\} \geqslant Pr\{|(Y - C - T)z| \leqslant r\} \geqslant \frac{1}{3}.$$

Note that the above inequality holds under the assumption $H_{j,\alpha}$, i.e.

$$Pr\{|s - t| \leqslant \frac{1}{g}|S| + r \mid H_{j,\alpha}\} \geqslant \frac{1}{3}.$$

Finally, we have the estimation

$$Pr\{|s - t| \leqslant \frac{1}{g}|S| + r\} \geqslant Pr\{|s - t| \leqslant \frac{1}{g}|S| + r,\ H_{j,\alpha}\}$$

$$= Pr\{|s - t| \leqslant \frac{1}{g}|S| + r \mid H_{j,\alpha}\} \cdot Pr\{H_{j,\alpha}\} \geqslant \frac{1}{3} \cdot \frac{\delta}{2m\beta} > 0.$$

This means $|s - t| \leqslant \frac{1}{g}|S| + r$ holds with a positive probability, so we complete the proof of Theorem 2.4.1. □

In the above proof, we have completed the whole process of transforming the INCGDD problem to the SIS problem, and prove that the difficulty of the INCGDD problem is polynomial equivalent with that of the SIS problem. This realizes the reduction principle from the worst case to the average case, which is the main result we introduce in this section. For hard problems on lattice, such as SIVP and GapSVP problems, based on Theorems 5.19, 5.22 and 5.23 in Micciancio and Regev (2004), we can transform them to the SIS problem equivalently. By Theorem 2.4.1, the difficulty of hard problem on lattice is polynomial equivalently with that of the SIS problem. In addition, the following Theorem 2.4.2 provides another way of reduction from SIVP to SIS problem.

**Theorem 2.4.2** (From SIVP to SIS) *Let the parameter $m$ be a polynomial function of $n$, i.e. $m = n^{O(1)}$, $\beta > 0$, $q \geqslant 2\beta n^{O(1)}$, $\gamma = \beta n^{O(1)}$, then the difficulty of solving the $SIS_{n,q,\beta,m}$ problem by a probabilistic polynomial algorithm is not lower than that of the $SIVP_\gamma$ problem.*

***Proof*** We are to prove that if there is a positive probability polynomial algorithm to get the solution of the $\mathrm{SIS}_{n,q,\beta,m}$ problem, so is the $\mathrm{SIVP}_\gamma$ problem. In other words, we can find $n$ linearly independent vectors $S = \{s_i\} \subset L$, such that $|S| = \max |s_i| \leqslant$

$\gamma(n)\lambda_n(L)$. Based on a set of linearly independent lattice vectors $S \subset L$ ($S$ is initially the generated matrix $B$ of lattice $L$), the idea of the reduction algorithm is using the oracle algorithm to obtain a set of new linearly independent lattice vectors $S' \subset L$ satisfying $|S'| \leqslant |S|/2$. Repeating this process and we can finally get the solution of the $\mathrm{SIVP}_\gamma$ problem. Let $q \geqslant 2\beta f(n)$, $f(n)$ be a polynomial function of $n$. We give the work process of this reduction algorithm.

1. According to the sampling lemma and combining lemma, generate $m$ short vectors $v_i \in L$ in the basic neighbourhood of lattice $L(S)$ such that $|v_i| \leqslant |S| f(n)$, $i = 1, 2, \ldots, m$, $V = [v_1, v_2, \ldots, v_m]$.

2. Let $A = B^{-1}V \pmod q$, by the combining lemma we know $A$ is uniformly distributed in $\mathbb{Z}_q^{n\times m}$. Solve the SIS problem $Az = 0 \pmod q$ with $|z| \leqslant \beta$ and obtain a solution $z$.

3. Let $s = Vz/q$. Repeat these three steps and generate enough vectors $s$ so that there are $n$ linearly independent vectors, denoted as $s_1, s_2, \ldots, s_n$. Suppose the matrix $S'$ is $S' = [s_1, s_2, \ldots, s_n]$.

We are to prove that $|S'| \leqslant |S|/2$. Firstly, note that $s \in L$. This is because

$$Vz = B(Az),\ \ Az = 0 \pmod q,$$

so $B(Az) \in qL$ and $s = Vz/q = B(Az)/q \in L$. Secondly,

$$|s| = |Vz|/q \leqslant |V|\beta/q \leqslant |S| f(n)\beta/(2\beta f(n)) = |S|/2.$$

This means $|S'| \leqslant |S|/2$. Replace $S$ with $S'$ and repeat the above three steps until $|S'| \leqslant \gamma(n)\lambda_n(L)$, then we confirm that $S'$ is a solution of the $\mathrm{SIVP}_\gamma$ problem. □

At the end of this section, we show that the difficulty of some other hard problems on lattice are polynomial equivalently with that of the SIS problems. We give another two definitions about hard problems on lattice.

**Definition 2.4.1** (1) $\mathrm{GIVP}_\gamma^\phi$: find a set of $n$ linearly independent vectors $S = \{s_i\} \subset L$, such that

$$|S| = \max |s_i| \leqslant \gamma(n)\phi(B), \tag{2.4.6}$$

where $\gamma(n) \geqslant 1$ is a positive function of $n$, $B$ is the generated matrix of $L$, and $\phi$ is a real function of $B$.

(2) $\mathrm{GDD}_\gamma^\phi$: let $t \in \mathbb{R}^n$ be a target vector, find a vector $x \in L$, such that

$$|x - t| \leqslant \gamma(n)\phi(B), \tag{2.4.7}$$

where $B$ is the generated matrix of $L$, and $\phi$ is a real function of $B$.

If $\phi = \lambda_n$ is the $n$th continuous minimal distance of lattice $L$, the $\mathrm{GIVP}_\gamma^\phi$ problem in the above definition becomes the $\mathrm{SIVP}_\gamma$ problem in Definition 2.2.3. Here we

give two lemmas to show that the above two problems could be reduced to the SIS problem.

**Lemma 2.4.1** *For any function $\gamma(n) \geqslant 1$ and $\phi$, there is a polynomial reduction algorithm from $GIVP_{8\gamma}^{\phi}$ to $INCGDD_{\gamma,8}^{\phi}$ problem.*

***Proof*** Suppose $B$ is a generated matrix of lattice $L$, our goal is to find a set of $n$ linearly independent vectors $S = \{s_i\} \subset L$ such that

$$|S| = \max |s_i| \leqslant 8\gamma(n)\phi(B).$$

We use the idea of iteration to achieve this goal. Initially, let $S = B$. If $S$ satisfies the above condition, then the solution has been found. If $S$ does not satisfy the above inequality, assume $S = [s_1, s_2, \ldots, s_n]$, and suppose that

$$|s_n| = \max_{1 \leqslant i \leqslant n} |s_i|,$$

i.e. $s_n$ is the longest vector among $s_1, s_2, \ldots, s_n$. Let $t$ be a vector orthogonal to $s_1, s_2, \ldots, s_{n-1}$, and $|t| = |S|/2 = |s_n|/2$. Here the vector $t$ can be constructed by the Schmidt orthogonalization method. Based on the reduction algorithm in Theorem 2.4.1, we solve the INCGDD problem with parameters $\{B, S, t, |S|/8\}$. If the algorithm fails, then we have

$$r = \frac{|S|}{8} \leqslant \gamma(n)\phi(B) \Rightarrow |S| \leqslant 8\gamma(n)\phi(B).$$

This implies $S$ is a solution of the $GIVP_{8\gamma}^{\phi}$ problem. If the reduction algorithm solves the INCGDD problem successfully, then we get a vector $u$, such that

$$|u - t| \leqslant \frac{|S|}{g} + r = \frac{|S|}{4}.$$

It follows that

$$|u| \leqslant |t| + \frac{|S|}{4} = \frac{3\,S|}{4}.$$

It is easy to verify $u, s_1, s_2, \ldots, s_{n-1}$ are linearly independent. Otherwise, $u$ is orthogonal to $t$ since $t$ is orthogonal to $s_1, s_2, \ldots, s_{n-1}$. Thus,

$$\frac{|S|^2}{16} \geqslant |u - t|^2 = |u|^2 + |t|^2 \geqslant |t|^2 = \frac{|S|^2}{4}.$$

It is a contradiction. So $u, s_1, s_2, \ldots, s_{n-1}$ are linearly independent. Let $S' = [s_1, s_2, \ldots, s_{n-1}, u]$, $|S'| < |S|$, repeat the above process for $S'$ and we get a solution of the $GIVP_{8\gamma}^{\phi}$ problem finally. Lemma 2.4.1 holds. □

**Lemma 2.4.2** *For any function $\gamma(n) \geqslant 1$ and $\phi$, there is a polynomial reduction algorithm from $GDD^{\phi}_{3\gamma}$ to $INCGDD^{\phi}_{\gamma,8}$ problem.*

***Proof*** Assume $B$ is a generated matrix of lattice $L$, $t \in \mathbb{R}^n$ is the target vector. Our goal is to find $x \in L$, such that

$$|x - t| \leqslant 3\gamma(n)\phi(B).$$

According to Lemma 2.4.1, we can find a set of $n$ linearly independent vectors $S = \{s_i\} \subset L$ such that $|S| \leqslant 8\gamma(n)\phi(B)$. Let $r$ be a real number satisfying the INCGDD problem with parameters $\{B, S, t, r/2\}$ fails, and $\{B, S, t, r\}$ successfully solves a solution $x$. In fact, the real number $r$ in this range $r/2 \leqslant \gamma(n)\phi(B) \leqslant r$ could satisfy the above condition. It follows that

$$|x - t| \leqslant \frac{|S|}{g} + r \leqslant \frac{|S|}{8} + 2\gamma(n)\phi(B) \leqslant 3\gamma(n)\phi(B).$$

So we get a solution of the $GDD^{\phi}_{3\gamma}$ problem. We complete the proof. □

In Lemma 2.4.1 and Lemma 2.4.2, we transform the $GIVP^{\phi}_{\gamma}$ and $GDD^{\phi}_{\gamma}$ problems to the $INCGDD^{\phi}_{\gamma,g}$ problem. While Theorem 2.4.1 tells us the difficulty of the $INCGDD^{\phi}_{\gamma,g}$ problem is polynomial equivalent with that of the SIS problem. So we have proved that the $GIVP^{\phi}_{\gamma}$ and $GDD^{\phi}_{\gamma}$ problems are polynomial equivalent with the SIS problem.



# Chapter 3
# Learning with Error


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 $n$,

$$T = \left(\begin{array}{c|c} 0 \ \cdots \ 0 & 1 \\ \hline & 0 \\ I_{n-1} & \vdots \\ & 0 \end{array}\right)_{n\times n}, \tag{3.1.1}$$

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.



Z. Zheng et al., *Modern Cryptography Volume 2*, Financial Mathematics and Fintech,
https://doi.org/10.1007/978-981-19-7644-5_3

$$e_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ e_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ \ldots, \ e_{n-1} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}. \tag{3.1.2}$$

Denote $e_m$ as $e_k$, if $m \equiv k \pmod{n}$, and $0 \leqslant k \leqslant n-1$, it is easy to see

$$Te_k = e_{k+1}, \text{ and } T^k(e_0) = e_k, \ 0 \leqslant k \leqslant n-1. \tag{3.1.3}$$

**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

$$T^*(\alpha) = [\alpha, T\alpha, \ldots, T^{n-1}\alpha]_{n\times n} \in \mathbb{R}^{n\times n}. \tag{3.1.4}$$

It is easy to verify that the circulant matrix $B$ generated by the linear combination vector is the linear combination of the corresponding circulant matrices, i.e.

$$T^*(a\alpha + b\beta) = aT^*(\alpha) + bT^*(\beta). \tag{3.1.5}$$

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

$$T^*(\alpha) = T^*\left(\sum_{i=0}^{n-1} \alpha_i e_i\right) = \sum_{i=0}^{n-1} \alpha_i T^*(e_i), \tag{3.1.6}$$

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

$$T^*(e_k) = T^k, \ 0 \leqslant k \leqslant n-1. \tag{3.1.7}$$

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* $\alpha = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix}$, $\beta = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{n-1} \end{pmatrix}$ *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)* $det(T^*(\alpha)) = \Pi_{i=0}^{n-1} \alpha(w_i)$, *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

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

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

and

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

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

$$\alpha(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1} \in \overline{R} \longleftrightarrow \alpha = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} \in \mathbb{R}^n, \tag{3.1.11}$$

written as $\alpha(x) \longleftrightarrow \alpha$ or $\alpha \longleftrightarrow \alpha(x)$. Then (3.1.11) gives a one-to-one correspondence between $\overline{R}$ and $\mathbb{R}^n$. In the same way, $\alpha(x) \longleftrightarrow \alpha$ 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

$$\alpha \otimes \beta = T^*(\alpha) \cdot \beta. \tag{3.1.12}$$

Under the above definition, $\mathbb{R}^n$, $\mathbb{Z}^n$ and $\mathbb{Z}_q^n$ become a commutative ring with unit element, respectively. Obviously, the convolution defined by (3.1.12) is closed on $\mathbb{Z}^n$ or $\mathbb{Z}_q^n$. 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 $\mathbb{Z}_q^n$. 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 $\mathbb{Z}_q^n$ 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 $\overline{R}$, $R$ and $R_q$ are defined by (3.1.8), (3.1.9) and (3.1.10), then we have the following three ring isomorphisms:*

$$\overline{R} \cong \mathbb{R}^n,\ R \cong \mathbb{Z}^n \text{ and } R_q \cong \mathbb{Z}_q^n.$$

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

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

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

$$\begin{aligned} x\beta(x) &= \beta_0 x + \beta_1 x^2 + \cdots + \beta_{n-2}x^{n-1} + \beta_{n-1}x^n \\ &= \beta_{n-1} + \beta_0 x + \cdots + \beta_{n-2}x^{n-1}, \end{aligned}$$

so $x\beta(x) \longleftrightarrow T\beta$. For all $k$, $0 \leqslant k \leqslant n-1$, 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 $\overline{R} \cong \mathbb{R}^n$. Similarly, we have $R \cong \mathbb{Z}^n$ and $R_q \cong \mathbb{Z}_q^n$. □

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

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

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

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

***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

$$|\alpha \otimes \beta| \leqslant \sqrt{n}|\alpha| \cdot |\beta|. \tag{3.1.15}$$

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

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

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

$$|b_i| \leqslant |\alpha| \cdot |\beta|, \ 1 \leqslant i \leqslant n.$$

It follows that

$$|\alpha \otimes \beta| = \left(\sum_{i=1}^{n} b_i^2\right)^{\frac{1}{2}} \leqslant \sqrt{n}|\alpha| \cdot |\beta|.$$

We complete the proof. □

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 $\alpha \in L$, $T\alpha \in L, \ldots, T^{n-1}\alpha \in L$, 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 $\alpha$. □

**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*

$$T^*(\alpha) = BD. \tag{3.1.16}$$

***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 $(0 \leqslant k \leqslant n-1)$

$$T^k\alpha = Bd_k,\ d_k \in \mathbb{Z}^n,\ D = [d_0, d_1, \ldots, d_{n-1}]_{n\times n} \in \mathbb{Z}^{n\times n},$$

the circulant matrix $T^*(\alpha)$ generated by $\alpha$ could be written as

$$T^*(\alpha) = [\alpha, T\alpha, \ldots, T^{n-1}\alpha] = [Bd_0, Bd_1, \ldots, Bd_{n-1}] = BD.$$

Lemma 3.1.5 holds. □

Let $L \subset \mathbb{R}^n$ be a lattice, for any $x \in \mathbb{R}^n$, there exists $u_x \in L \Rightarrow$

$$|x - u_x| = \min_{\alpha\in L, \alpha\neq x} |\alpha - x| = |x - L|. \tag{3.1.17}$$

$u_x$ is called the nearest lattice vector of $x$. We define the covering radius $\rho(L)$ of $L$ by

$$\rho(L) = \max_{x\in\mathbb{R}^n} |x - u_x| = \max_{x\in\mathbb{R}^n} |x - L|. \tag{3.1.18}$$

Obviously, the covering radius $\rho(L)$ satisfies that any sphere $N(x, \rho(L))$ with radius $\rho(L)$ contains at least one lattice vector. If $L_1 \subset L$ is a sublattice, then for any $x \in \mathbb{R}^n$,

$$|x - L| \leqslant |x - L_1| \Rightarrow \rho(L) \leqslant \rho(L_1). \tag{3.1.19}$$

If $L = L(B)$, we write $\rho(L) = \rho(B)$. The final goal of this section is to prove the existence of the covering radius and give an upper bound estimate of $\rho(L)$ using Babai's nearest plane algorithm.

Let $L = L(B)$, $S = \{s_1, s_2, \ldots, s_n\} \subset L$ be $n$ linearly independent lattice vectors. $S^* = \{s_1^*, s_2^*, \ldots, s_n^*\}$ is the orthogonal basis corresponding to $S$ by the Gram-Schmidt method. We define

$$\sigma(S) = \left(\sum_{i=1}^{n} |s_i^*|^2\right)^{\frac{1}{2}}. \tag{3.1.20}$$

**Lemma 3.1.6** *(Babai) Let $L = L(B) \subset \mathbb{R}^n$ be a full rank lattice, $S \subset L$ be the set of $n$ linearly independent lattice vectors, then for any $t \in \mathbb{R}^n$, there exists a lattice vector $w \in L \Rightarrow$*

$$|t - w| \leqslant \frac{1}{2}\sigma(S). \tag{3.1.21}$$

*Specially, the covering radius $\rho(L)$ of $L$ exists and satisfies $\rho(L) \leqslant \frac{1}{2}\sigma(S)$.*

***Proof*** Without loss of generality, we only prove for the case $S = B$. Since $L(S) \subset L(B)$ is a full rank sublattice, by (3.1.21) $w \in L(S) \Rightarrow w \in L(B)$ and $\rho(L) \leqslant \rho(S) \leqslant \frac{1}{2}\sigma(S)$. Let $B = [\beta_1, \beta_2, \ldots, \beta_n]$, the corresponding orthogonal basis is $B^* = [\beta_1^*, \beta_2^*, \ldots, \beta_n^*]$. Babai's algorithm is based on the following two techniques:

(1) Rounding off (see Theorem 7 of Chap. 7 in Zheng (2022))

$\forall x \in \mathbb{R}^n$, 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

$$[x]_B = \sum_{i=1}^{n} \delta_i \beta_i^*,\ \{x\}_B = \sum_{i=1}^{n} a_i \beta_i^*,\ -\frac{1}{2} < a_i \leqslant \frac{1}{2},\ 1 \leqslant i \leqslant n.$$

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))

$$\begin{cases} U = L(\beta_1, \beta_2, \ldots, \beta_{n-1}) = L(\beta_1^*, \beta_2^*, \ldots, \beta_{n-1}^*) \\ v = \delta_n \beta_n \in L \\ x' = \sum\limits_{i=1}^{n-1} x_i \beta_i^* + \delta_n \beta_n^* \\ y \text{ is the nearest lattice vector of } x - v \text{ in } L' \\ w = y + v \in L \end{cases} . \tag{3.1.22}$$

Since $v = \delta_n \beta_n$, $x' = \sum_{i=1}^{n-1} x_i \beta_i^* + \delta_n \beta_n^*$,

$$|x - x'| = |x_n - \delta_n||\beta_n^*| \leqslant \frac{1}{2}|\beta_n^*|.$$

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

$$|x - x'| \leqslant |x - u_x|.$$

Let $w = y + v = y + \delta_n \beta_n \in L$, we are to prove

$$|x - w|^2 = |x - x'|^2 + |x' - w|^2. \tag{3.1.23}$$

This is because

$$x - x' = (x_n - \delta_n)\beta_n^*,\ x' - w = x' - v - y \in U,$$

therefore,

$$(x - x')\perp(x' - w),$$

and (3.1.23) holds. Based on the assumption:

$$|x' - w|^2 \leqslant \frac{1}{4}\left(|\beta_1^*|^2 + \cdots + |\beta_{n-1}^*|^2\right).$$

It follows that

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

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

$$|t - w| \leqslant \frac{1}{2}\sigma(B).$$

This lemma holds. □

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

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

$$\rho(L) \leqslant r \leqslant \gamma(n)\rho(L). \tag{3.1.24}$$

## 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 $\mathbb{Z}_q[x]$

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

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. $A = (a_1(x), \ldots, a_m(x)) \in R_q^m$, with the norm $|A|$ defined by

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

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

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

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

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

$$f_A(z) = \sum_{i=1}^{m} a_i(x) z_i(x) \equiv 0 \ (\mathrm{mod}\ x^n - 1),$$

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

**Remark 3.2.2** In order to guarantee the $R_q - \mathrm{SIS}_{q,\beta,m}$ 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 $z_i(x) \longleftrightarrow z_i \in \mathbb{Z}_q^n$, 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 $R_q - \mathrm{SIS}_{q,\beta,m}$:**

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

$$\begin{cases} f_A(z) = \sum_{i=1}^{m} a_i \otimes z_i = 0 \\ |z_i| \leqslant \sqrt{n},\ 1 \leqslant i \leqslant n \end{cases}. \tag{3.2.4}$$

Obviously, $R_q -$ 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 $R$, $X \subset R$, $|X| = 2^n$, $b \in R$ 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

$$f_A(z) = \sum_{i=1}^{m} a_i z_i = b, \ \forall z_i \in X. \tag{3.2.5}$$

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 $R = R_q$, $b = 0$, then the above problem becomes the SIS problem on $R_q$. The main result in this section is the following theorem:

**Theorem 3.2.1** *Let $m = O(\log n)$, $k = \tilde{O}(\log n)$, $q \geqslant 4mkn^{\frac{5}{2}}$, and $\gamma \geqslant 16mkn^3$, if we can solve the knapsack problem (3.2.6) on $R_q$, then there exists a probabilistic polynomial algorithm solving the covering radius problem $CDP_\gamma$ for any n dimensional full rank cyclic lattice.*

The knapsack problem on $R_q$ in Theorem 3.2.1 is the more general case of (3.2.4), which is summarized in the following definition.

**Knapsack problem on** $R_q$: Choose $m$ vectors $A = (a_1, a_2, \ldots, a_m)$ uniformly distributed on $\mathbb{Z}_q^n$ randomly and any target vector $b \in \mathbb{Z}_q^n$, find a set of short vectors $z = (z_1, z_2, \ldots, z_m)$ such that

$$f_A(z) = \sum_{i=1}^{m} a_i \otimes z_i = b, \ |z_i| \leqslant \sqrt{n}, \ 1 \leqslant i \leqslant m. \tag{3.2.6}$$

From Theorem 3.2.1, the knapsack problem on $R_q$ 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 $L = L(B) \subset \mathbb{R}^n$ under the assumption that (3.2.6) is solvable, where $S = \{s_1, s_2, \ldots, s_n\} \subset L$ 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 $|s_i^*| \leqslant |s_i|$ $(1 \leqslant i \leqslant n)$, we have

$$\sigma(S) = \left(\sum_{i=1}^{n} |s_i^*|^2\right)^{\frac{1}{2}} \leqslant \left(\sum_{i=1}^{n} |s_i|^2\right)^{\frac{1}{2}}. \tag{3.2.7}$$

By Lemma 3.1.6, $\rho(L) \leqslant \frac{1}{2}\sigma(S)$. 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

$$|S| = |s_n| = \max_{1 \leqslant i \leqslant n} |s_i|.$$

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

$$|s'| \leqslant \frac{1}{2}|s_n| = \frac{1}{2}|S|,$$

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

$$|S'| \leqslant \frac{1}{2}|S|. \tag{3.2.8}$$

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

$$|S| \leqslant \frac{2\gamma}{\sqrt{n}}\rho(L), \tag{3.2.9}$$

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

$$\rho(L) \leqslant \frac{1}{2}\sigma(S) \leqslant \frac{\sqrt{n}}{2}|S| \leqslant \gamma\rho(L).$$

So we complete solving the $\mathrm{CDP}_\gamma$ problem.

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

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

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

$$\sigma(S) > 2\gamma\rho(L). \tag{3.2.11}$$

To find $s'$ in the reduced algorithm, by Lemma 3.1.6, there is a lattice vector $c \in L \Rightarrow$

$$|c - \beta e_0| \leqslant \frac{1}{2}\sigma(S). \tag{3.2.12}$$

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 $0 \leqslant k \leqslant n-1$,

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

Note that $T^k e_0 = e_k$, so

$$|T^k c - \beta e_k| \leqslant \frac{1}{2}\sigma(S).$$

Because $c \in L$ and $L$ is a cyclic lattice, then $T^k c \in L$ $(0 \leqslant k \leqslant n-1)$. 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 $qe_j$ $(0 \leqslant j \leqslant n-1) \in L(B') \Rightarrow q\mathbb{Z}^n \subset L(B')$. □

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

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

Let

$$a_i \equiv \sum_{j=1}^{k} w_{ij}^{'} \ (\mathrm{mod}\ q) \Rightarrow a_i \in \mathbb{Z}_q^n, \tag{3.2.14}$$

$A = (a_1, a_2, \ldots, a_m)$ contains the above $m$ vectors in $\mathbb{Z}_q^n$, consider the knapsack problem on $R_q = (\mathbb{Z}_q^n, +, \otimes)$,

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

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

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

where

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

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

$$\begin{cases} x_{ij} = \frac{1}{q} T^*(c) x_{ij}^{'} \text{ and } w_{ij} = \frac{1}{q} T^*(c) w_{ij}^{'} \\ s' = \sum\limits_{i=1}^{m} \sum\limits_{j=1}^{k} (x_{ij} - w_{ij}) \otimes (y_i - \hat{y}_i) \end{cases}. \tag{3.2.17}$$

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 $L$ ($1 \leqslant i \leqslant m, 1 \leqslant j \leqslant k$), 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

$$x_{ij} = \frac{1}{q} T^*(c) B'\alpha = \frac{1}{q} T^*(c) \cdot q(T^*(c))^{-1} \cdot B\alpha = B\alpha \in L(B).$$

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

$$\begin{aligned} s' &= \sum x_{ij} \otimes (y_{ij} - \hat{y}_{ij}) - \sum w_{ij} \otimes (y_{ij} - \hat{y}_{ij}) \\ &= \sum T^*(x_{ij})(y_{ij} - \hat{y}_{ij}) - \sum T^*(w_{ij})(y_{ij} - \hat{y}_{ij}) \\ &= \sum_{i=1}^{m} T^*(\sum_{j=1}^{k} x_{ij})(y_i - \hat{y}_i) - \sum_{i=1}^{m} T^*(\sum_{j=1}^{k} w_{ij})(y_i - \hat{y}_i). \end{aligned} \tag{3.2.18}$$

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 $w_{ij}$,

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

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

$$\begin{aligned}\sum_{i=1}^{m} T^*(\sum_{j=1}^{k} w_{ij})(y_i - \hat{y}_i) &= \frac{1}{q}T^*(c)\sum_{i=1}^{m} T^*(\sum_{j=1}^{k} w_{ij}^{'})(y_i - \hat{y}_i) \\ &= \frac{1}{q}T^*(c)\sum_{i=1}^{m}\sum_{j=1}^{k} w_{ij}^{'} \otimes (y_i - \hat{y}_i).\end{aligned} \tag{3.2.19}$$

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.

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

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*

$$|s'| \leqslant \frac{1}{2}|s_n| = \frac{1}{2}|S|. \tag{3.2.20}$$

***Proof*** We only prove $|s'| \leqslant \sigma(S)/2\sqrt{n}$, since

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

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

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

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 $|\alpha| \leqslant \frac{1}{2}\sigma(S)$ (see (3.2.12)), and

$$\begin{aligned} x_{ij} - w_{ij} &= \frac{1}{q}(\alpha + \beta e_0) \otimes (x_{ij}^{'} - w_{ij}^{'}) = \frac{1}{q}T^*(\alpha + \beta e_0)(x_{ij}^{'} - w_{ij}^{'}) \\ &= \frac{1}{q}\beta T^*(e_0)(x_{ij}^{'} - w_{ij}^{'}) + \frac{1}{q}T^*(\alpha)(x_{ij}^{'} - w_{ij}^{'}) \\ &= \frac{\beta}{q}(x_{ij}^{'} - w_{ij}^{'}) + \frac{1}{q}T^*(\alpha)(x_{ij}^{'} - w_{ij}^{'}). \end{aligned}$$

Since

$$|x_{ij}^{'} - w_{ij}^{'}| \leqslant \frac{1}{2}\sqrt{n},$$

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

$$\begin{aligned} |x_{ij} - w_{ij}| &\leqslant \frac{\beta}{q}|x_{ij}^{'} - w_{ij}^{'}| + \frac{1}{q}|\alpha \otimes (x_{ij}^{'} - w_{ij}^{'})| \\ &\leqslant \frac{\beta}{q} \cdot \frac{1}{2}\sqrt{n} + \frac{1}{q} \cdot \frac{\sqrt{n}}{2} \cdot \sqrt{n} \cdot \frac{1}{2}\sigma(S) \\ &= \frac{\beta}{q} \cdot \frac{\sqrt{n}}{2} + \frac{1}{q}\sqrt{n} \cdot \frac{\sigma(S)}{2} \cdot \frac{\sqrt{n}}{2} \\ &= \sigma(S)\left(\frac{2n^{\frac{3}{2}}}{\gamma} + \frac{n}{2q}\right) \\ &\leqslant \sigma(S)\left(\frac{1}{8} \cdot \frac{1}{mkn^{\frac{3}{2}}} + \frac{1}{8} \cdot \frac{1}{mkn^{\frac{3}{2}}}\right) \\ &= \frac{1}{4}\sigma(S)\frac{1}{mkn^{\frac{3}{2}}}. \end{aligned}$$

Based on (3.2.21), we get

$$|s'| \leqslant mk\sqrt{n} \max_{i,j} |x_{ij} - w_{ij}| \cdot \max_{i} |y_i - \hat{y}_i|$$

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

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*

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

*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. $|t' - L(B')| \geqslant \rho(B')$, and

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

Denote

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

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

$$\begin{aligned} \rho(B) &\geqslant \operatorname{dist}(t, L(B)) = |t - Bz_0| \\ &= |\frac{1}{q} T^*(c)t' - Bz_0| = |\frac{1}{q} T^*(c)(t' - B'z_0)| \\ &\geqslant \frac{1}{q} |t' - B'z_0| \min_{d} \frac{|c \otimes d|}{|d|} \\ &\geqslant \frac{1}{q} \rho(B') \min_{d \in \mathbb{R}^n, d \neq 0} \frac{|c \otimes d|}{|d|}. \end{aligned} \tag{3.2.22}$$

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 $|\alpha| \leqslant \frac{1}{2}\sigma(S)$, so

$$\begin{aligned} |c \otimes d| &= |(\beta e_0 + \alpha) \otimes d| \\ &\geqslant |d|(\beta - \frac{1}{2}\sqrt{n}\sigma(S)) \\ &\geqslant \beta|d| - \sqrt{n}|\alpha||d| \\ &= |d|\frac{4nq}{\gamma}\sigma(S). \end{aligned}$$

By (3.2.22), we have (see (3.2.11))

$$\begin{aligned} \rho(B) &\geqslant \frac{1}{q}\rho(B') \cdot \frac{4nq}{\gamma}\sigma(S) \\ &\geqslant 8n\rho(B')\rho(B). \end{aligned}$$

This implies $\rho(B') \leqslant \frac{1}{8n}$. Lemma 3.2.4 holds. □

**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 $r \geqslant \rho(\Lambda)$. Then the number of lattice vectors of $L(B)$ contained in $Q$ satisfies*

$$\frac{Vol(Q)}{det(\Lambda)}(1 - \frac{\rho(\Lambda)n}{\gamma}) \leqslant |L(B) \cap Q| \leqslant \frac{Vol(Q)}{det(\Lambda)}(1 + \frac{2\rho(\Lambda)n}{\gamma}).$$

***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

$$a_{ij} \equiv w_{ij}^{'} \pmod{q}, \ a_i \equiv \sum_{j=1}^{k} a_{ij} \pmod{q}, \tag{3.2.23}$$

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 $\rho(L(B')) \leqslant \frac{1}{8n} < \frac{1}{2}$, from lemma 3.2.4, the number $N$ of lattice vectors of $L(B')$ in this cube satisfies

$$\frac{1}{\det(B')}\left(1 - \frac{1}{4}\right) \leqslant N \leqslant \frac{1}{\det(B')}(1 + \frac{1}{2}).$$

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,

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

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 $x \in G$,*

$$\left|Pr\{A_i = x\} - \frac{1}{|G|}\right| \leqslant \frac{1}{2|G|}.$$

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

$$\Delta(\xi, U(G)) \leqslant 2^{-(k+1)}.$$

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

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

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

$$\begin{aligned}
\left|\Pr\{\xi = x\} - \frac{1}{|G|}\right| &= \left|\sum_{a\in G} Pr\{\xi' = a, A_k = x - a\} - \frac{1}{|G|}\right| \\
&= \left|\sum_{a\in G} \Pr\{\xi' = a\}\Pr\{A_k = x - a\} - \frac{1}{|G|}\right| \\
&= \left|\sum_{a\in G} \left(\Pr\{\xi' = a\} - \frac{1}{|G|}\right)\left(\Pr\{A_k = x - a\} - \frac{1}{|G|}\right)\right| \\
&\leqslant \sum_{a\in G} \frac{1}{2^{k-1}|G|} \cdot \frac{1}{2|G|} = \frac{1}{2^k|G|}.
\end{aligned}$$

Thus,

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

This lemma holds. □

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, $n \geqslant 1$ and $\varepsilon \geqslant 0$ be a given parameter. The distribution of $\xi$ with parameter $\varepsilon$ on $\mathbb{Z}_2$ is

$$\Pr\{\xi = 0\} = 1 - \varepsilon, \ \Pr\{\xi = 1\} = \varepsilon.$$

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

$$\begin{cases} b_1 \equiv_\varepsilon < a_1, s > \pmod 2 \\ b_2 \equiv_\varepsilon < a_2, s > \pmod 2 \\ \vdots \\ b_m \equiv_\varepsilon < a_m, s > \pmod 2 \end{cases}, \tag{3.3.1}$$

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 $n \geqslant 1$, $q \geqslant 2$ 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

$$\Pr\{a \equiv b + e \pmod{q}\} = \chi(e), \tag{3.3.2}$$

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

$$a \equiv_\chi b + e \pmod{q}, \text{ or } a =_\chi b + e. \tag{3.3.3}$$

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 $\mathbb{Z}_q$:

$$b \equiv a_1 s_1 + a_2 s_2 + \cdots + a_n s_n \pmod{q},$$

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

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

$\mathbb{Z}_q$, $e_i \leftarrow \chi$, the $\mathrm{LWE}_{n,q,\chi,m}$ 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

$$\begin{cases} b_1 =_\chi < a_1, s > +e_1 \\ b_2 =_\chi < a_2, s > +e_2 \\ \vdots \\ b_m =_\chi < a_m, s > +e_m \end{cases}. \tag{3.3.4}$$

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

$$\begin{cases} b_1 \equiv < a_1, s > \pmod q \\ b_2 \equiv < a_2, s > \pmod q \\ \vdots \\ b_m \equiv < a_m, s > \pmod q \end{cases}.$$

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 $\mathrm{LWE}_{n,q,\chi,m}$ 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

$$b \equiv_\chi A's + e \pmod q, \tag{3.3.5}$$

where $A'$ 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

$\chi(e_i)$, so

$$\Pr\{b \equiv_\chi A's + e \pmod q\} = \Pi_{i=1}^m \chi(e_i) = \chi(e). \tag{3.3.6}$$

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:

$$\begin{cases} \Lambda_q(A) = \{A'x \mid x \in \mathbb{Z}_q^n\} + q\mathbb{Z}_q^n \\ \Lambda_q^\perp(A) = \{x \in \mathbb{Z}_q^m \mid Ax \equiv 0 \pmod q\} \end{cases}. \tag{3.3.7}$$

Since $\Lambda_q(A) = q\Lambda_q^\perp(A)^*$, $A's \in \Lambda_q(A)$, the geometric meaning of $\mathrm{LWE}_{n,q,\chi,m}$ 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,

$$\begin{cases} b_1 \equiv_\chi A_1's + e_1 \pmod q \\ b_2 \equiv_\chi A_2's + e_2 \pmod q \end{cases}.$$

Let $A_1^* = (A_1')^{-1}$, and

$$\overline{b} = \begin{pmatrix} A_1^* b_1 \\ A_1^* b_2 \end{pmatrix},\ \overline{e} = \begin{pmatrix} A_1^* e_1 \\ A_1^* e_2 \end{pmatrix}.$$

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. □

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, $z \equiv x + y \ (mod\ q)$. If $x$ is uniformly distributed on $\mathbb{Z}_q$, so is $z$.*

***Proof*** For any integer $0 \leqslant i \leqslant q-1$, we compute the probability that $z$ takes the value $i$.

$$\begin{aligned}\Pr\{z=i\} &= \sum_{j=0}^{q-1} Pr\{x=j, y=i-j\} \\ &= \sum_{j=0}^{q-1} Pr\{x=j\}Pr\{y=i-j\} \\ &= \frac{1}{q}\sum_{j=0}^{q-1} Pr\{y=i-j\} = \frac{1}{q}.\end{aligned}$$

□

**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),

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

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 $\mathbb{T} \equiv [0, 1)\ (\text{mod } 1)$ of length 1, with the density function

$$\psi_\beta(x) = \sum_{k=-\infty}^{+\infty} \frac{1}{\beta} e^{-\frac{\pi}{\beta^2}(x-k)^2},\ x \in \mathbb{T}. \tag{3.3.9}$$

It is easy to see that

$$\int_{\mathbb{T}} \psi_\beta(x)\mathrm{d}x = \int_0^1 \psi_\beta(x)\mathrm{d}x = \int_{\mathbb{R}} \frac{1}{\beta}\rho_\beta(x)\mathrm{d}x = 1.$$

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*

$$|x| \leqslant t,\ \textit{and}\ |x - y| \leqslant l.$$

*Then*

$$\rho_s(y) \geqslant \left(1 - \frac{\pi}{s^2}(2tl + l^2)\right)\rho_s(x). \tag{3.3.10}$$

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

$$e^{-z} \geqslant 1 - z,\ z \in \mathbb{R}.$$

Therefore,

$$\begin{aligned}\rho_s(y) &= e^{-\frac{\pi}{s^2}|y|^2} \geqslant e^{-\frac{\pi}{s^2}(|x|+|y-x|)^2}\\ &\geqslant e^{-\frac{\pi}{s^2}(|x|^2+2l|x|+l^2)}\\ &\geqslant e^{-\frac{\pi}{s^2}(|x|^2+2tl+l^2)}\\ &\geqslant (1 - \frac{\pi}{s^2}(2tl + l^2))\rho_s(x).\end{aligned}$$

□

**Lemma 3.3.5** *Let $0 < \alpha < \beta \leqslant 2\alpha$, then the statistical distance between $\psi_\alpha$ and $\psi_\beta$ satisfies*

$$\Delta(\psi_\alpha, \psi_\beta) \leqslant \frac{9}{2}(\frac{\beta}{\alpha} - 1). \tag{3.3.11}$$

***Proof*** Based on

$$\int_0^1 \psi_\beta(x)\mathrm{d}x = 1,$$

it follows that

$$
\begin{aligned}
&\int_0^1 |\psi_\beta(x) - \psi_\alpha(x)| \mathrm{d}x \\
&= \int_0^1 \left| \sum_{k=-\infty}^{+\infty} \left( \frac{1}{\beta} e^{-\frac{\pi}{\beta^2}|k-x|^2} - \frac{1}{\alpha} e^{-\frac{\pi}{\alpha^2}|k-x|^2} \right) \right| \mathrm{d}x \\
&\leqslant \sum_{k=-\infty}^{+\infty} \int_0^1 \left| \frac{1}{\beta} e^{-\frac{\pi}{\beta^2}|x-k|^2} - \frac{1}{\alpha} e^{-\frac{\pi}{\alpha^2}|x-k|^2} \right| \mathrm{d}x \\
&= \int_{-\infty}^{+\infty} \left| \frac{1}{\beta} e^{-\frac{\pi}{\beta^2}|x|^2} - \frac{1}{\alpha} e^{-\frac{\pi}{\alpha^2}|x|^2} \right| \mathrm{d}x.
\end{aligned}
$$

Let $x = \alpha y$, we get

$$
\int_0^1 |\psi_\beta(x) - \psi_\alpha(x)| \mathrm{d}x \leqslant \int_{-\infty}^{+\infty} \left| \frac{1}{\beta/\alpha} e^{-\frac{\pi}{(\beta/\alpha)^2}|y|^2} - e^{-\pi|y|^2} \right| \mathrm{d}y. \tag{3.3.12}
$$

Without loss of generality, assume $\alpha = 1$, $\beta = 1 + \varepsilon$, where $0 < \varepsilon \leqslant 1$, we estimate the right hand of (3.3.12)

$$
\begin{aligned}
&\int_{\mathbb{R}} \left| e^{-\pi|x|^2} - \frac{1}{1+\varepsilon} e^{-\frac{\pi}{(1+\varepsilon)^2}|x|^2} \right| \mathrm{d}x \\
&\leqslant \int_{\mathbb{R}} \left| e^{-\pi|x|^2} - e^{-\frac{\pi}{(1+\varepsilon)^2}|x|^2} \right| \mathrm{d}x + \int_{\mathbb{R}} (1 - \frac{1}{1+\varepsilon}) e^{-\frac{\pi}{(1+\varepsilon)^2}|x|^2} \mathrm{d}x \\
&= \int_{\mathbb{R}} \left| e^{-\pi|x|^2} - e^{-\frac{\pi}{(1+\varepsilon)^2}|x|^2} \right| \mathrm{d}x + \varepsilon \\
&= \int_{\mathbb{R}} \left| 1 - e^{-\pi(1-\frac{1}{(1+\varepsilon)^2})x^2} \right| \cdot e^{-\frac{\pi}{(1+\varepsilon)^2}x^2} \mathrm{d}x + \varepsilon.
\end{aligned}
$$

For $\forall z \geqslant 0$, we have

$$
1 - z \leqslant e^{-z} \leqslant 1 \Rightarrow 0 \leqslant 1 - e^{-z} \leqslant z,
$$

and

$$
\begin{aligned}
\left| e^{-\pi(1-\frac{1}{(1+\varepsilon)^2})x^2} - 1 \right| &\leqslant \pi(1 - \frac{1}{(1+\varepsilon)^2})x^2 \\
&= \frac{\pi}{(1+\varepsilon)^2}(2\varepsilon + \varepsilon^2)x^2 \leqslant 2\pi\varepsilon x^2.
\end{aligned}
$$

Finally,

$$\int_0^1 |\psi_\alpha(x) - \psi_\beta(x)|\mathrm{d}x \leqslant 2\pi\varepsilon \int_{\mathbb{R}} x^2 e^{-\frac{\pi}{(1+\varepsilon)^2}x^2}\mathrm{d}x + \varepsilon = \varepsilon + \varepsilon(1+\varepsilon)^3 \leqslant 9\varepsilon.$$

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

$$\Delta(\psi_\alpha, \psi_\beta) = \frac{1}{2}\int_0^1 |\psi_\alpha(x) - \psi_\beta(x)|\mathrm{d}x \leqslant \frac{9}{2}(\frac{\beta}{\alpha} - 1).$$

We complete the proof of this lemma. □

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

$$\mathbb{T} \equiv [0, 1) \ (\mathrm{mod}\ 1).$$

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

$$\overline{\varphi} = \lfloor q\varphi \rceil, \tag{3.3.13}$$

that is, if $\varphi$ takes a value $x \in \mathbb{T}$, then $\overline{\varphi}$ takes the value $\lfloor qx \rceil \bmod q$, where $\lfloor x \rceil$ is the closest integer to $x$. When $x$ runs over $[0, 1)$, obviously $\lfloor qx \rceil$ 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*

$$Pr\{\overline{\varphi} = k\} = \overline{\varphi}(k) = \int_{(k-\frac{1}{2})/q}^{(k+\frac{1}{2})/q} \varphi(x)\mathrm{d}x, \ k \in \mathbb{Z}_q.$$

***Proof***

$$\Pr\{\overline{\varphi} = k\} = Pr\{\lfloor q\varphi \rceil = k\} = \Pr\left\{k - \frac{1}{2} \leqslant q\varphi < k + \frac{1}{2}\right\}$$

$$= \Pr\left\{\left(k - \frac{1}{2}\right)/q \leqslant \varphi < \left(k + \frac{1}{2}\right)/q\right\} = \int_{(k-\frac{1}{2})/q}^{(k+\frac{1}{2})/q} \varphi(x)\mathrm{d}x.$$

□

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

$$\overline{\psi}_\beta(k) = \int_{(k-\frac{1}{2})/q}^{(k+\frac{1}{2})/q} \psi_\beta(x)\mathrm{d}x, \tag{3.3.14}$$

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 $m = Poly(n)$, $q \leqslant 2^{Poly(n)}$, $\chi = \overline{\psi}_\alpha$ be the discrete Gauss distribution with parameter $\alpha$, where $0 < \alpha < 1$, and $\alpha q \geqslant 2\sqrt{n}$. Then the difficulty of solving the D-LWE$_{n,q,\chi,m}$ problem is at least as hard as that of GapSVP$_\gamma$ or 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 LWE$_{n,q,\chi,m}$ problem is as least as hard as difficult problems on any lattice such as the GapSVP and SIVP problems.*

*(2) Prove the difficulty of the D-LWE$_{n,q,\chi,m}$ problem is not lower than that of the LWE$_{n,q,\chi,m}$ problem (see Theorem 3.4.1 in the next section). The original proof 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 $q = 2^{Poly(n)}$ (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 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 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.

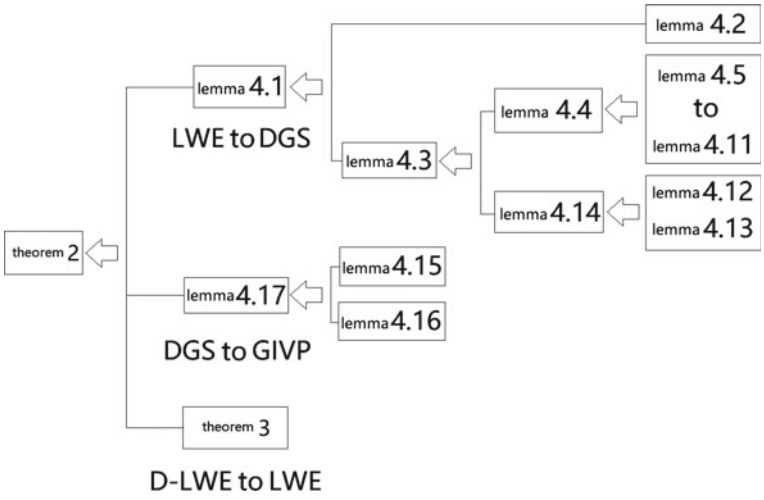


**Fig. 3.1** The flowchart of the proof of Theorem 3.3.1

**Definition 3.4.1** $\mathrm{DGS}_\phi$: 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 $\mathrm{DGS}_{\sqrt{2n}\eta_\varepsilon(L)/\alpha}$ problem. In Sect. 3.4.2, we give a reduction algorithm from the $\mathrm{GIVP}_{2\sqrt{n}\phi}$ problem to the $\mathrm{DGS}_\phi$ 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 $\text{D-LWE}_{n,q,\chi,m}$ can be reduced to the $\mathrm{LWE}_{n,q,\chi,m}$ 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 $\mathrm{DGS}_{\sqrt{2n}\eta_\varepsilon(L)/\alpha}$ problem by the algorithm of $\mathrm{LWE}_{n,q,\psi_\alpha,m}$ 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 $m = Poly(n)$, $\varepsilon = \varepsilon(n)$ be a negligible function of $n$, $q = q(n)$ be a positive integer, $\alpha = \alpha(n) \in (0, 1)$, $\alpha q \geqslant 2\sqrt{n}$, $\chi = \psi_\alpha$. Assume that we have an algorithm $W$ that solves the $LWE_{n,q,\psi_\alpha,m}$ problem given a polynomial number of samples, then there exists an efficient quantum algorithm for the $DGS_{\sqrt{2n}\eta_\varepsilon(L)/\alpha}$ problem.*

**Lemma 3.4.2** *For any $n$ dimensional lattice $L$ and a real number $r > 2^{2n}\lambda_n(L)$, 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 $m = Poly(n)$, $\varepsilon = \varepsilon(n)$ be a negligible function of $n$, $q = q(n) \geqslant 2$ be a positive integer, $\alpha = \alpha(n) \in (0, 1)$. Assume that we have an algorithm $W$ that solves the $LWE_{n,q,\psi_\alpha,m}$ 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 $r > \sqrt{2}q\eta_\varepsilon(L)$ and $n^c$ samples from $D_{L,r}$, outputs a sample from $D_{L,r\sqrt{n}/(\alpha q)}$.*

**Proof of Lemma** 3.4.1: Given an $n$ dimensional lattice $L$ and a real number $r > \sqrt{2n}\eta_\varepsilon(L)/\alpha$, 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

$$r_i = r(\alpha q/\sqrt{n})^i, \quad i = 1, 2, \ldots, 3n.$$

Based on Lemma 1.3.6 in Chap. 1,

$$r_{3n} > 2^{3n}r > 2^{3n}\sqrt{2n}\eta_\varepsilon(L)/\alpha \geqslant 2^{3n}\sqrt{2n}\sqrt{\frac{\ln 1/\varepsilon}{\pi}}\frac{\lambda_n(L)}{n} > 2^{2n}\lambda_n(L).$$

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 $D_{L,r_{3n}\sqrt{n}/(\alpha q)}$, i.e. $D_{L,r_{3n-1}}$. Repeat this process, since

$$r_1 = r\alpha q/\sqrt{n} > \sqrt{2n}\eta_\varepsilon(L)/\alpha \cdot \alpha q/\sqrt{n} = \sqrt{2}q\eta_\varepsilon(L),$$

which satisfies the condition of Lemma 3.4.3, finally we can output a sample from $D_{L,r_1\sqrt{n}/(\alpha q)} = D_{L,r}$. 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 $b_i \leqslant 2^n\lambda_n(L)$, $1 \leqslant i \leqslant n$. 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

$$D_r(x) = \frac{\rho_r(x)}{r^n}, \ \forall x \in \mathbb{R}^n.$$

We get $y' = y \bmod L \in F(B)$, 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

$$|y'| \leqslant \mathrm{diam}(F(B)) \leqslant \sum_{i=1}^{n} |b_i| \leqslant n2^n \lambda_n(L),$$

where

$$\mathrm{diam}(F(B)) = \max\{|u - v| \mid u, v \in F(B)\}.$$

Based on Lemma 1.3.4 in Chap. 1,

$$\rho(L \backslash \sqrt{n} r N) < (r\sqrt{2\pi e} e^{-\pi r^2})^n \rho(L),$$

here $N$ is the unit ball. This means $\rho(L \backslash \sqrt{n} r N)$ is exponentially small, so we can always assume $x \leqslant \sqrt{n} r$. By Lemma 3.3.4, let $t = \sqrt{n} r$, $l = n2^n \lambda_n(L)$, by some simple calculations we get

$$\begin{aligned} \Pr\{\xi = x\} &= \int\limits_{x+F(B)} D_r(y)\mathrm{d}y \geqslant \int\limits_{x+F(B)} (1 - 2^{-\Omega(n)}) D_r(x)\mathrm{d}y \\ &= (1 - 2^{-\Omega(n)}) D_r(x)\det(L). \end{aligned}$$

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

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

So we have

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

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

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

$$|u - t| = \min_{x \in L, |x-t| \leqslant d} |x - t|.$$

(2) $\mathrm{CVP}_{L,d}^{(q)}$: given an $n$ dimensional lattice $L$ with generated matrix $B$, a target vector $t \in \mathbb{R}^n$, a real number $d$, $\mathrm{dist}(t, L) \leqslant d$, denote $K_L(t) = \{u \in L \mid |u - t| = \min\limits_{x \in L} |x - t|\}$, i.e. $K_L(t)$ is the closest vector to $t$ in the lattice $L$, output $B^{-1} K_L(t) \bmod q \in \mathbb{Z}_q^n$.

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 $\mathrm{CVP}_{L^*,\alpha q/(\sqrt{2}r)}$ problem, and Lemma 3.4.14 shows that we can generate a sample of $D_{L,r\sqrt{n}/\alpha q}$ from the algorithm of solving the $\mathrm{CVP}_{L^*,\alpha q/(\sqrt{2}r)}$ 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 $\mathrm{CVP}_{L^*,\alpha q/(\sqrt{2}r)}$ 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 $\mathrm{CVP}_{L^*,\alpha q/(\sqrt{2}r)}$ to $D_{L,r\sqrt{n}/\alpha q}$.

**Lemma 3.4.4** *Let $m = Poly(n)$, $\varepsilon = \varepsilon(n)$ be a negligible function of $n$, $q = q(n) \geqslant 2$ be a positive integer, $\alpha = \alpha(n) \in (0, 1)$. Assume that we have an algorithm $W$ that solves $LWE_{n,q,\psi_\alpha,m}$ 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 $CVP_{L^*,\alpha q/(\sqrt{2}r)}$ 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 $\mathrm{CVP}^{(q)}$ problems.

**Lemma 3.4.5** *Given an $n$ dimensional lattice $L$, a real number $d < \lambda_1(L)/2$, $q \geqslant 2$ is a positive integer. There exists an efficient algorithm to solve the $CVP_{L,d}$ problem based on the algorithm for $CVP^{(q)}_{L,d}$.*

***Proof*** Let $x \in \mathbb{R}^n$ satisfying $\mathrm{dist}(x, L) \leqslant d$ be the target vector, define vectors $\{x_n\}$ and $\{a_n\}$ as follows: $x_1 = x$,

$$a_i = B^{-1}K_L(x_i) \in \mathbb{Z}^n,\ i \geqslant 1,$$

which is the coefficient vector of the closest vector to $x_i$ in lattice $L$,

$$x_{i+1} = (x_i - B(a_i \bmod q))/q,\ i \geqslant 1,$$

it is easy to prove

$$a_{i+1} = (a_i - (a_i \bmod q))/q,$$

and

$$|x_{i+1} - Ba_{i+1}| \leqslant \frac{d}{q^i}.$$

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

$$a_{i+1} = (a_i - (a_i \bmod q))/q,$$

we get $a_n, a_{n-1}, \ldots, a_1$, and complete the process of solving the $\mathrm{CVP}_{L,d}$ 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 $\mathbb{T} = [0, 1)$, 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 $\mathbb{T}$ with density function $\phi$. The LWE distribution $A_{s,\phi} = (a, b) \in \mathbb{Z}_q^n \times \mathbb{T}$ generated by $s$ and $\phi$ satisfies:
(1) $a \in \mathbb{Z}_q^n$ is uniformly distributed.
(2) $b = a \cdot s/q + e \bmod 1$.

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

**Lemma 3.4.6** *Let $q = q(n) \geqslant 1$ 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 $A_{s,\psi_\alpha}$, $\mathbb{T} = [0, 1)$, $\xi$ be a random variable on $\mathbb{T}$ 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 $1 \leqslant j \leqslant n$, 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 $a_j(s_j - s_j') \bmod q$ has period $g$, i.e. the distribution of $a_j(s_j - s_j')/q \bmod 1$ has period $g/q = 1/k$, $k \geqslant 2$. Since $\xi$ is regarded as the sum of $a_j(s_j - s_j')/q \bmod 1$ and an independent random variable, therefore, the distribution of $\xi$ also has period $1/k$. Assume $\tilde{z}$ is the expectation of $\cos(2\pi\xi)$,

$$\tilde{z} = E[\cos(2\pi\xi)] = \int_0^1 \cos(2\pi y)p(y)\mathrm{d}y = \mathrm{Re}\int_0^1 e^{2\pi iy}p(y)\mathrm{d}y.$$

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 $e^{2\pi iy}p(y)$ with period 1 is fixed in any interval of length 1, then

$$\begin{aligned}\int_0^1 e^{2\pi iy}p(y)\mathrm{d}y &= \int_{\frac{1}{k}}^{1+\frac{1}{k}} e^{2\pi iy}p(y)\mathrm{d}y \\ &= \int_0^1 e^{2\pi i(y+\frac{1}{k})}p(y)\mathrm{d}y \\ &= e^{\frac{2\pi i}{k}}\int_0^1 e^{2\pi iy}p(y)\mathrm{d}y.\end{aligned}$$

From $k \geqslant 2$ we know $\tilde{z} = 0$, by the Chebyshev inequality,

$$Pr\{|z - \tilde{z}| \leqslant 0.01\} \geqslant 1 - \frac{\mathrm{Var}[\cos(2\pi\xi)]}{0.01^2 n}.$$

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

Based on Lemma 3.4.6 and the algorithm for $\mathrm{LWE}_{n,q,\psi_\alpha,m}$, for any $\beta \leqslant \alpha$ 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 $q = q(n) \geqslant 2$ 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 $\beta \leqslant \alpha$ 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

$\psi_{\sqrt{\gamma}}$ to the second component of each sample from $A_{s,\psi_\beta}$, so we obtain $n^c$ samples from $A_{s,\psi_{\sqrt{\beta^2+\gamma}}}$. 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

$$\Gamma = \min\{\gamma \in Z, \gamma \geqslant \alpha^2 - \beta^2\}.$$

From the definition of the set $Z$

$$\Gamma \leqslant \alpha^2 - \beta^2 + n^{-2c}\alpha^2.$$

Let $\alpha' = \sqrt{\beta^2 + \Gamma}$, we have

$$\alpha \leqslant \alpha' \leqslant \sqrt{\alpha^2 + n^{-2c}\alpha^2} \leqslant (1 + n^{-2c})\alpha.$$

Based on lemma 3.3.5,

$$\Delta(\psi_\alpha, \psi_{\alpha'}) \leqslant \frac{9}{2}\left(\frac{\alpha'}{\alpha} - 1\right) \leqslant \frac{9}{2}n^{-2c}.$$

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 $1 - 9n^{-c} \geqslant \frac{1}{2}$. 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, $c \in \mathbb{R}^n$, $\varepsilon > 0$, $r \geqslant \eta_\varepsilon(L)$, we have*

$$\rho_r(L + c) \in r^n det(L^*)(1 \pm \varepsilon). \tag{3.4.2}$$

***Proof*** Based on Lemma 1.3.2 in Chap. 1,

$$\begin{aligned}\rho_r(L + c) &= \sum_{x\in L} \rho_{r,-c}(x) = \det(L^*) \sum_{y\in L^*} \hat{\rho}_{r,-c}(y) \\ &= r^n \det(L^*) \sum_{y\in L^*} e^{2\pi i c\cdot y} \rho_{1/r}(y) \\ &= r^n \det(L^*)(1 + \sum_{y\in L^*\setminus\{0\}} e^{2\pi i c\cdot y} \rho_{1/r}(y)).\end{aligned}$$

From $r \geqslant \eta_\varepsilon(L)$, it follows that $\rho_{1/r}(L^*\setminus\{0\}) \leqslant \varepsilon$, and

$$\left|\sum_{y\in L^*\setminus\{0\}} e^{2\pi ic\cdot y}\rho_{1/r}(y)\right| \leqslant \sum_{y\in L^*\setminus\{0\}} \rho_{1/r}(y) \leqslant \varepsilon.$$

We get

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

The proof is complete. □

**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 $rs/t = 1/\sqrt{1/r^2+1/s^2} \geqslant \eta_\varepsilon(L)$, let $\xi$ be the sum of a discrete Gauss distribution $D_{L+u,r}$ and a noise distribution $D_s$, then*

$$\Delta(\xi, D_t) \leqslant 2\varepsilon. \tag{3.4.3}$$

***Proof*** Let the density function of $\xi$ be $Y(x)$, then

$$\begin{aligned}
Y(x) &= \frac{1}{s^n\rho_r(L+u)}\sum_{y\in L+u}\rho_r(y)\rho_s(x-y)\\
&= \frac{1}{s^n\rho_r(L+u)}\sum_{y\in L+u}\exp\left(-\pi\left(\left|\frac{y}{r}\right|^2+\left|\frac{x-y}{s}\right|^2\right)\right)\\
&= \frac{1}{s^n\rho_r(L+u)}\sum_{y\in L+u}\exp\left(-\pi\left(\frac{r^2+s^2}{r^2s^2}\left|y-\frac{r^2}{r^2+s^2}x\right|^2+\frac{1}{r^2+s^2}|x|^2\right)\right)\\
&= \exp\left(-\frac{\pi}{r^2+s^2}|x|^2\right)\frac{1}{s^n\rho_r(L+u)}\\
&\quad\sum_{y\in L+u}\exp\left(-\pi\left(\frac{r^2+s^2}{r^2s^2}\left|y-\frac{r^2}{r^2+s^2}x\right|^2\right)\right)\\
&= \frac{\rho_t(x)}{s^n}\frac{\rho_{rs/t,(r/t)^2x-u}(L)}{\rho_{r,-u}(L)}\\
&= \frac{\rho_t(x)}{s^n}\frac{\hat{\rho}_{rs/t,(r/t)^2x-u}(L^*)}{\hat{\rho}_{r,-u}(L^*)}\\
&= \frac{\rho_t(x)}{t^n}\frac{(t/rs)^n\hat{\rho}_{rs/t,(r/t)^2x-u}(L^*)}{(1/r)^n\hat{\rho}_{r,-u}(L^*)}.
\end{aligned} \tag{3.4.4}$$

Based on the Fourier transform property of Gauss function in Lemma 1.2.1 in Chap. 1, we get

$$\hat{\rho}_{rs/t,(r/t)^2x-u}(w) = \exp(-2\pi i((r/t)^2x-u)\cdot w)(rs/t)^n\rho_{t/rs}(w),$$

and

$$\hat{\rho}_{r,-u}(w) = \exp(2\pi i u \cdot w) r^n \rho_{1/r}(w).$$

Since $r \geqslant \frac{rs}{t} \geqslant \eta_\varepsilon(L)$,

$$|1 - (t/rs)^n \hat{\rho}_{rs/t,(r/t)^2 x-u}(L^*)| \leqslant \rho_{t/rs}(L^* \backslash \{0\}) \leqslant \varepsilon,$$

$$|1 - (1/r)^n \hat{\rho}_{r,-u}(L^*)| \leqslant \rho_{1/r}(L^* \backslash \{0\}) \leqslant \varepsilon.$$

It follows that

$$1 - 2\varepsilon \leqslant \frac{1-\varepsilon}{1+\varepsilon} \leqslant \frac{(t/rs)^n \hat{\rho}_{rs/t,(r/t)^2 x-u}(L^*)}{(1/r)^n \hat{\rho}_{r,-u}(L^*)} \leqslant \frac{1+\varepsilon}{1-\varepsilon} \leqslant 1 + 4\varepsilon.$$

By (3.4.4),

$$|Y(x) - \frac{\rho_t(x)}{t^n}| \leqslant 4\varepsilon \frac{\rho_t(x)}{t^n}.$$

Integrate for $x \in \mathbb{R}^n$,

$$\Delta(\xi, D_t) = \frac{1}{2} \int_{\mathbb{R}^n} |Y(x) - \frac{\rho_t(x)}{t^n}| \mathrm{d}x \leqslant 2\varepsilon.$$

We complete the proof. □

**Lemma 3.4.10** *For any $n$ dimensional lattice $L$, vectors $z, u \in \mathbb{R}^n$, real numbers $r, \alpha > 0$, $\varepsilon < \frac{1}{2}$, $\eta_\varepsilon(L) \leqslant 1/\sqrt{1/r^2 + (|z|/\alpha)^2}$, 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*

$$\Delta(z \cdot v + e, \xi) \leqslant 2\varepsilon. \tag{3.4.5}$$

*In particular,*

$$\Delta(z \cdot v + e \mod 1, \psi_{\sqrt{(r|z|)^2+\alpha^2}}) \leqslant 2\varepsilon. \tag{3.4.6}$$

***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 $2\varepsilon$,

$$\Delta(v + h, D_{\sqrt{r^2+(\alpha/|z|)^2}}) \leqslant 2\varepsilon.$$

By the property of statistical distance,

$$\Delta(z \cdot (v+h), z \cdot D_{\sqrt{r^2+(\alpha/|z|)^2}}) \leqslant 2\varepsilon.$$

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.

$$\Delta(z \cdot v + e, \xi) \leqslant 2\varepsilon,$$

mod 1 for both of the two random variables,

$$\Delta(z \cdot v + e \bmod 1, \psi_{\sqrt{(r|z|)^2+\alpha^2}}) \leqslant 2\varepsilon.$$

The lemma holds. □

**Lemma 3.4.11** *Let $\varepsilon = \varepsilon(n)$ be a negligible function of $n$, $q = q(n) \geqslant 2$ 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 $A_{s,\psi_\beta}$ for any $\beta \leqslant \alpha$ ($\beta$ is unknown), then there exists an efficient algorithm that given an $n$ dimensional lattice $L$, a real number $r > \sqrt{2}q\eta_\varepsilon(L)$ 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 $x \in \mathbb{R}^n$, $\mathrm{dist}(x, L^*) \leqslant \alpha q/(\sqrt{2}r)$, denote the generated matrix of $L$ is $B$, and the generated matrix of $L^*$ is $(B^T)^{-1}$, our goal is to solve $s = B^T K_{L^*}(x) \bmod q$. The idea of algorithm $W'$ is to generate a polynomial number of samples from $A_{s,\psi_\beta}$, 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 $D_{L,r}$, $a = B^{-1}v \bmod q$, $e$ be random variable of Gauss distribution with mean 0 and standard deviation $\alpha/(2\sqrt{\pi})$, then there is $\beta \leqslant \alpha$ such that the statistical distance between $(a, x \cdot v/q + e \bmod 1)$ and $A_{s,\psi_\beta}$ 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 $q\eta_\varepsilon(L) < r$, 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 $x \cdot v/q + e \bmod 1$. Let $x' = x - K_{L^*}(x)$, from $\mathrm{dist}(x, L^*) \leqslant \alpha q/(\sqrt{2}r)$ we get $|x'| \leqslant \alpha q/(\sqrt{2}r)$ and

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

We compute the distributions of $K_{L^*}(x) \cdot v/q \bmod 1$ 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,

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

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

$$1/\sqrt{1/r^2 + (\sqrt{2}|x'|/\alpha q)^2} \geqslant r/\sqrt{2} > q\eta_\varepsilon(L) = \eta_\varepsilon(qL)$$

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), $x \cdot v/q + e \bmod 1$ and $\psi_\beta + s \cdot a/q \bmod 1$ have the same distribution. Above all, we get the statistical distance between $(a, x \cdot v/q + e \bmod 1)$ and $A_{s,\psi_\beta}$ is negligible so that the algorithm $W'$ is correct. We complete the proof. □

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 $\mathrm{CVP}_{L^*,\alpha q/(\sqrt{2}r)}$ problem by the samples of $D_{L,r}$. 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 $D_{L,r\sqrt{n}/\alpha q}$ based on the algorithm for the $\mathrm{CVP}_{L^*,\alpha q/(\sqrt{2}r)}$ 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

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

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*

$$\sum_{x\in L}\sqrt{\rho_r(x)}|x\rangle = \sum_{x\in L}\rho_{\sqrt{2}r}(x)|x\rangle. \tag{3.4.9}$$

*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*

$$v_1 = \sum_{x\in L/R, |x|<\sqrt{n}} \rho(x)|x \bmod L\rangle. \tag{3.4.10}$$

*and*

$$\begin{aligned} v_2 &= \sum_{x\in L/R} \rho(x)|x \bmod L\rangle \\ &= \sum_{L/R\cap F}\sum_{y\in L}\rho(x-y)|x\rangle. \end{aligned} \tag{3.4.11}$$

*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 $\mathrm{CVP}_{L^*,d}$ 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 $r > \sqrt{2}q\eta_\varepsilon(L)$, we have

$$\frac{\alpha q}{\sqrt{2}r} < \frac{\alpha}{2\eta_\varepsilon(L)} \leqslant \frac{\alpha}{2}\sqrt{\frac{\pi}{\ln(1/\varepsilon)}}\lambda_1(L^*) < \frac{\lambda_1(L^*)}{2},$$

replace $d$ in Lemma 3.4.14 with $\alpha q/(\sqrt{2}r)$, then there exists a quantum algorithm to generate a sample from the discrete Gauss distribution $D_{L,r\sqrt{n}/\alpha q}$ given the algorithm for the $\mathrm{CVP}_{L^*,\alpha q/(\sqrt{2}r)}$ problem.

Combine Lemma 3.4.4 with Lemma 3.4.14, for $r > \sqrt{2}q\eta_\varepsilon(L)$, we have proved that one can solve the $\mathrm{CVP}_{L^*,\alpha q/(\sqrt{2}r)}$ problem given the algorithm for the $\mathrm{LWE}_{n,q,\psi_\alpha,m}$ problem and a polynomial number of samples from $D_{L,r}$, and further to generate a sample from $D_{L,r\sqrt{n}/\alpha q}$, 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 $\mathrm{LWE}_{n,q,\psi_\alpha,m}$ problem to solve the $\mathrm{DGS}_{\sqrt{2n}\eta_\varepsilon(L)/\alpha}$ 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

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

where $\gamma(n) \geqslant 1$ 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 $L \subset \mathbb{R}^n$, $\varepsilon \leqslant \frac{1}{10}$, $r \geqslant \sqrt{2}\eta_\varepsilon(L)$, 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*

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

***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

$$
\begin{aligned}
&\underset{x\sim D_{L,r}}{E}[e^{-\pi(x_1/r)^2}] \\
&= \frac{1}{\rho_r(L)}\sum_{x\in L} e^{-\pi(\sqrt{2}x_1/r)^2} e^{-\pi(x_2/r)^2}\cdots e^{-\pi(x_n/r)^2} \\
&= \frac{\det(L^*)r^n}{\sqrt{2}\rho_r(L)}\sum_{y\in L^*} e^{-\pi(ry_1/\sqrt{2})^2} e^{-\pi(ry_2)^2}\cdots e^{-\pi(ry_n)^2} \\
&\leqslant \frac{\det(L^*)r^n}{\sqrt{2}\rho_r(L)}\rho_{\sqrt{2}/r}(L^*),
\end{aligned}
$$

where $y = (y_1, y_2, \ldots, y_n) \in L^*$. Since $r/\sqrt{2} \geqslant \eta_\varepsilon(L)$, we get

$$\rho_{\sqrt{2}/r}(L^*) = 1 + \rho_{\sqrt{2}/r}(L^*\backslash\{0\}) \leqslant 1 + \varepsilon.$$

It follows that

$$\underset{x\sim D_{L,r}}{E}[e^{-\pi(x_1/r)^2}] \leqslant \frac{\det(L^*)r^n}{\sqrt{2}\rho_r(L)}(1+\varepsilon).$$

By Lemma 1.3.2 in Chap. 1 again,

$$\rho_r(L) = \det(L^*)r^n\rho_{1/r}(L^*) \geqslant \det(L^*)r^n,$$

therefore,

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

On the other hand,

$$
\begin{aligned}
\underset{x\sim D_{L,r}}{E}[e^{-\pi(x_1/r)^2}] &\geqslant \sum_{x\in H, x\sim D_{L,r}} \frac{\rho_r(x)}{\rho_r(L)}[e^{-\pi(x_1/r)^2}] \\
&= \sum_{x\in H, x\sim D_{L,r}} \frac{\rho_r(x)}{\rho_r(L)} = Pr\{x \in H\}.
\end{aligned}
$$

According to the above two inequalities,

$$\Pr\{x \in H\} \leqslant \frac{9}{10},$$

that is,

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

The lemma holds. □

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 $L \subset \mathbb{R}^n$, $\varepsilon \leqslant \frac{1}{10}$, $r \geqslant \sqrt{2}\eta_\varepsilon(L)$, 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

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

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

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

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,

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

Thus,

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

that is,

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

It follows that

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

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. □

Based on the above preparations, let's prove the main conclusion in this subsection.

**Lemma 3.4.17** *Given an n dimensional lattice $L$, $\varepsilon = \varepsilon(n) \leqslant \frac{1}{10}$, $\phi(L) \geqslant \sqrt{2}\eta_\varepsilon(L)$, if there exists an algorithm for the DGS$_\phi$ 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 $s_i \leqslant 2^n \lambda_n(L)$, $1 \leqslant i \leqslant n$. Let

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

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

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

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 DGS$_\phi$ problem, and the corresponding sets of $n^2$ vectors are denoted as $S_0, S_1, \ldots, S_{2n}$. If $\tilde{\lambda}_n \leqslant \phi(L)$, we have

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

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 $\phi(L) \leqslant r_i \leqslant 2\phi(L)$ according to Lemma 1.3.6 in Chap. 1,

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

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 $\phi(L) \leqslant r_i \leqslant 2\phi(L)$. 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 $\sqrt{n}r_i \leqslant 2\sqrt{n}\phi(L)$ is close to 1. Let $V = [v_1, v_2, \ldots, v_n]$, we get $|V| \leqslant 2\sqrt{n}\phi(L)$, so we find a solution of the GIVP$_{2\sqrt{n}\phi}$ problem. This lemma holds. □

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 DGS 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 DGS 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 $n \geqslant 1$ be a positive integer, $2 \leqslant q \leqslant Poly(n)$ 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.

# Chapter 4
# LWE Public Key Cryptosystem


In 2005, O.Regev proposed the first LWE public key cryptosystem at Tel Aviv University in Israel based on LWE distribution $A_{s,\chi}$. Because of this paper, Regev won the highest award for theoretical computer science in 2018—the Godel Award. The size of public key is $\tilde{O}(n^2)$ bits, and the size of private key $s$ and ciphertext is $\tilde{O}(n)$ bits. The plaintext encrypted each time is 1 bit. In fact, the LWE public key cryptosystem is a probabilistic cryptosystem, which depends on a high probability algorithm. Since the security of LWE problem has been clearly proved (see Chap. 3), the LWE cryptosystem has received extensive attention as soon as it was proposed, and it becomes the most cutting-edge research topic in the lattice-based cryptosystem study.

## 4.1 LWE Cryptosystem of Regev

Let $n \geqslant 1, q \geqslant 2$ be positive integers, $\chi$ be a given probability distribution in $\mathbb{Z}_q$. By Definition 4.3.1 in Chap. 3, the LWE distribution $A_{s,\chi}$ is

$$\begin{cases} A_{s,\chi} = (a, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q, \\ b \equiv_\chi < a, s > +e \pmod{q}, \end{cases} \tag{4.1.1}$$

where $a \in \mathbb{Z}_q^n$ is uniformly distributed, $s \in \mathbb{Z}_q^n$ is the private key chosen at random, $e \in \mathbb{Z}_q$, $e \leftarrow \chi$ is called error distribution. LWE cryptosystem depends on LWE distribution $A_{s,\chi}$, and its workflow has the following three steps:

(1) Public key.

First we choose $s \in \mathbb{Z}_q^n$ at random as the private key, let $m = O(n\log q)$. Then we choose $m$ samples distributed from $A_{s,\chi}$, $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, $e_i \in \mathbb{Z}_q$, $e_i \leftarrow \chi$, $1 \leqslant i \leqslant m$. Let

$$\overline{A} = [a_1, a_2, \ldots, a_m]_{n\times m} \in \mathbb{Z}_q^{n\times m},$$



Z. Zheng et al., *Modern Cryptography Volume 2*, Financial Mathematics and Fintech,
https://doi.org/10.1007/978-981-19-7644-5_4

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}, \ e = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix}, \ e \leftarrow \chi^m,$$

where $\overline{A}$ is a matrix uniformly at random, $e \leftarrow \chi^m$ indicates the $m$ samples are independent. The public key of LWE cryptosystem is the following $(n+1) \times m$ matrix

$$A = \begin{pmatrix} \overline{A} \\ b' \end{pmatrix} \in \mathbb{Z}_q^{(n+1)\times m}. \tag{4.1.2}$$

If the uniformly random matrix $\overline{A}$ is given and saved for all the users of LWE cryptosystem, then the true public key is $b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{Z}_q^m$ with size $O(m) = \tilde{O}(n)$.

The public key and private key satisfy the following equation:

$$(-s', 1)A \equiv_\chi e' \ (\mathrm{mod}\ q). \tag{4.1.3}$$

(2) Encryption.

In order to encrypt plaintext of 1 bit $u \in \mathbb{Z}_2$, let $x \in \{0,1\}^m$ be an uniformly distributed $m$ dimensional vector with each entry 0 or 1. The ciphertext $c \in \mathbb{Z}_q^{n+1}$ is an $(n+1)$ dimensional vector in $\mathbb{Z}_q$, defined by

$$f_A(u) = c = Ax + \begin{pmatrix} 0 \\ u \cdot \lfloor \frac{q}{2} \rceil \end{pmatrix} \in \mathbb{Z}_q^{n+1}, \tag{4.1.4}$$

where $0 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{Z}_q^n$, $u\lfloor \frac{q}{2} \rceil \in \mathbb{Z}_q$, $\lfloor \frac{q}{2} \rceil$ is the nearest integer to $\frac{q}{2}$. We call $f_A$ the encryption algorithm of LWE. In order to understand the encryption algorithm better, we give another definition of $f_A$.

The following set $\{1, 2, \ldots, m\}$ has $2^m$ subsets. We choose a subset $S \subset \{1, 2, \ldots, m\}$ uniformly at random which is called the index set. Then the encryption algorithm $f_A(u)$ for plaintext $u \in \mathbb{Z}_2$ is

$$c = f_A(u) = \begin{pmatrix} \sum_{i\in S} a_i \\ \sum_{i\in S} b_i + u\lfloor \frac{q}{2} \rceil \end{pmatrix} \in \mathbb{Z}_q^{n+1}. \tag{4.1.5}$$

In fact, the subset $S$ is corresponding to the uniformly chosen vector $x \in \{0,1\}^m$. The above algorithm (4.1.5) was proposed by Regev originally.

(3) Decryption.

We use the private key $s \in \mathbb{Z}_q^n$ for decryption of the ciphertext $c$. Actually we only need to decrypt for the last entry of vector $c$. We have

$$f_A^{-1}(c) = (-s', 1)c = (-s', 1)Ax + u\lfloor\frac{q}{2}\rceil \equiv_\chi e'x + u\lfloor\frac{q}{2}\rceil \pmod q. \tag{4.1.6}$$

The error samples are much smaller than $q$, namely

$$\sum_{i\in S} e_i = e'x < \lfloor\frac{q}{2}\rceil/2. \tag{4.1.7}$$

Therefore, by comparing the distances between the right side of (4.1.6) and 0 or $\lfloor\frac{q}{2}\rceil$, one can decrypt successfully:

$$f_A^{-1}(c) = \begin{cases} 0, & \text{if } (-s', 1)c \text{ is closer to } 0, \\ 1, & \text{if } (-s', 1)c \text{ is closer to } \lfloor\frac{q}{2}\rceil, \end{cases} \tag{4.1.8}$$

finally we have $f_A^{-1}(c) = u$ and finish the whole workflow of LWE cryptosystem.

Both of the encryption algorithm and decryption algorithm of LWE are probabilistic algorithms, so we should verify the correctness, namely

$$Pr\{f_A^{-1}(c) = u\} \geqslant 1 - \delta(n). \tag{4.1.9}$$

Here $\delta(n)$ is a negligible function of $n$, i.e. $\delta(n) = o\left(\frac{1}{\log^\epsilon n}\right), \forall \epsilon > 0$, more precisely:

$$\lim_{n\to\infty} \delta(n)\log^\epsilon n = 0, \ \forall \epsilon > 0.$$

We prove (4.1.9) with given discrete Gauss distribution $\chi = \overline{\psi}_\alpha$. For $a \in \mathbb{Z}_q$, $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$,

$$|a| = \begin{cases} a, & \text{if } 0 < a \leqslant \lfloor\frac{q}{2}\rceil, \\ q - a, & \text{if } \lfloor\frac{q}{2}\rceil < a \leqslant q - 1. \end{cases} \tag{4.1.10}$$

For $x \in \mathbb{T} = [0, 1)$, we define

$$|x| = \begin{cases} x, & \text{if } 0 \leqslant x < \frac{1}{2}, \\ 1 - x, & \text{if } \frac{1}{2} \leqslant x < 1. \end{cases} \tag{4.1.11}$$

**Lemma 4.1.1** *Let $\delta > 0$, $0 \leqslant k \leqslant m$, if the distribution $\chi^k$ satisfies*

$$\Pr_{e\sim\chi^k}\left\{|e| < \lfloor\frac{q}{2}\rceil/2\right\} > 1 - \delta, \tag{4.1.12}$$

*then (4.1.9) holds, i.e.*

$$Pr\left\{f_A^{-1}(c) = u\right\} > 1 - \delta.$$

***Proof*** When we choose the error samples $e_i \in \mathbb{Z}_q$, $e_i \leftarrow \chi$, we can always guarantee $e_i = |e_i|$ without changing the probability distribution. By (4.1.7), suppose that $|S| = k$, the corresponding sample

$$e = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{pmatrix}, \ |e| = \sum_{i=1}^{k} |e_i| = \sum_{i=1}^{k} e_i.$$

As long as (4.1.7) holds, i.e.

$$|e| < \lfloor \frac{q}{2} \rceil / 2 \Rightarrow f_A^{-1}(c) = u,$$

then

$$Pr\left\{f_A^{-1}(c) = u\right\} \geqslant Pr\left\{|e| < \lfloor \frac{q}{2} \rceil / 2\right\} > 1 - \delta.$$

□

Next we prove (4.1.12) holds for discrete Gauss distribution $\overline{\psi}_\alpha$ in $\mathbb{Z}_q$. The following assumptions are made for the selection of parameters:

$$\begin{cases} n \geqslant 1, \ q \geqslant 2, \ n^2 \leqslant q \leqslant 2n^2, \\ m = (1+\epsilon)(n+1)\log q, \ \epsilon > 0 \text{ is any positive real number}, \\ \chi = \overline{\psi}_{\alpha(n)}, \ \alpha(n) = o(\frac{1}{\sqrt{n}\log n}), \end{cases} \tag{4.1.13}$$

where the symbol $o$ indicates

$$\lim_{n \to 0} \alpha(n)\sqrt{n}\log n = 0.$$

For example, we can choose $\alpha(n) = \frac{1}{\sqrt{n}\log^2 n}$, or

$$\alpha(n) = \left(\sqrt{n}\log^{1+\epsilon} n\right)^{-1}, \ \forall \epsilon > 0.$$

**Lemma 4.1.2** *Under the condition for parameters of (4.1.13), for any $0 \leqslant k \leqslant m$, we have*

$$\underset{e \sim \overline{\psi}_{\alpha(n)}^k}{Pr}\left\{|e| < \lfloor \frac{q}{2} \rceil / 2\right\} > 1 - \delta(n), \tag{4.1.14}$$

*where $\delta(n) = o\left(\frac{1}{log^\epsilon n}\right)$, $\forall \epsilon > 0$, is a negligible function.*

***Proof*** Based on (4.1.13), when $n \geqslant n_0$, it is easy to see that

$$0 \leqslant k \leqslant m \leqslant 4(1+\epsilon)(n+1)\log n < \frac{n^2}{32} \leqslant \frac{q}{32}.$$

The $k$ samples $e = \begin{pmatrix} e_1 \\ \vdots \\ e_k \end{pmatrix}$ distributed as $\overline{\psi}_\alpha^k$ could be obtained from the $k$ samples $x_1, x_2, \ldots, x_k$ of distribution $\psi_\alpha$, where

$$x_i \in \left[0, \frac{1}{2}\right), \ e_i = \lfloor q x_i \rceil \bmod q, \ 1 \leqslant i \leqslant k.$$

Here the set of representative elements of $\mathbb{Z}_q$ is

$$\mathbb{Z}_q = \left\{ a \in \mathbb{Z} \mid -\frac{q}{2} \leqslant a < \frac{q}{2} \right\}.$$

So we have

$$|e| = \sum_{i=1}^{k} |e_i| = \sum_{i=1}^{k} \lfloor q x_i \rceil \bmod q.$$

Note that

$$\sum_{i=1}^{k} (\lfloor q x_i \rceil - q x_i) \bmod q \leqslant k \leqslant \frac{q}{32}.$$

Therefore,

$$\sum_{i=1}^{k} q x_i \bmod q \leqslant \frac{q}{16} \Rightarrow \left(\sum_{i=1}^{k} x_i\right) \bmod 1 \leqslant \frac{1}{16},$$

we have $|e| < \lfloor \frac{q}{2} \rceil / 2$. Since $\sum_{i=1}^{k} x_i \bmod 1$ distributed as $\psi_{\sqrt{k}\alpha}$, where $\sqrt{k} \cdot \alpha = o\left(\frac{1}{\sqrt{\log n}}\right)$, so

$$Pr\left\{ \sum_{i=1}^{k} x_i \bmod 1 < \frac{1}{16} \right\} = 1 - \delta(n),$$

where $\delta(n) = \sqrt{k} \cdot \alpha = o\left(\frac{1}{\sqrt{\log n}}\right)$. We complete the proof. □

## 4.2 The Proof of Security

To prove the security of Regev's cryptosystem, we first prove some general properties for the probability distribution of Abel group by Impagliazzo and Zurkerman Impagliazzo and Zuckerman (1989).

Let $G$ be a finite Abel group, $k \geqslant 1$ be a positive integer. For any $l$ elements $g_1, g_2, \ldots, g_l \in G$, suppose $x \in \{0,1\}^l$, $g = (g_1, g_2, \ldots, g_l)$, then

$$gx = \sum_{i=1}^{l} x_i g_i, \ x_i = 0 \text{ or } 1$$

is called a subsum of $\{g_1, g_2, \ldots, g_l\}$. Randomly choose $x \in \{0,1\}^l$, let $gx$ denote the distribution of subsum, and let $U(G)$ denote the uniformly distribution on $G$.

**Lemma 4.2.1** *For any $l$ elements $\{g_1, g_2, \ldots, g_l\}$ uniformly at random, the expectation of statistical distance between the distribution of subsum and the uniformly distribution on $U(G)$ is*

$$E(\Delta(gx, U(G))) \leqslant (|G|/2^l)^{\frac{1}{2}}.$$

*Specially, the probability that the statistical distance is larger than $(|G|/2^l)^{\frac{1}{4}}$ is no more than $(|G|/2^l)^{\frac{1}{4}}$, i.e.*

$$Pr\left\{\Delta(gx, U(G)) \geqslant (|G|/2^l)^{\frac{1}{4}}\right\} \leqslant (|G|/2^l)^{\frac{1}{4}}.$$

***Proof*** Let $g = (g_1, g_2, \ldots, g_l)$ be $l$ group elements chosen at random, $h \in G$ is a given group element. Define $P_g(h)$

$$P_g(h) = \frac{1}{2^l}\left|\left\{x \in \{0,1\}^l \mid gx = \sum_{i=1}^{l} x_i g_i = h\right\}\right|,$$

we call $P_g(h)$ the distribution of subsum for $g$. In order to prove $P_g(h)$ is close to uniformly distribution, we first prove the $l_2$ norm between $P_g(h)$ and the uniformly distribution is very small. In fact, we have:

$$\sum_{h \in G} P_g(h)^2 = \Pr_{x,x'}\{gx = gx'\} = \frac{1}{2^l} + \Pr_{x,x'}\{gx = gx', \ x \neq x'\}.$$

Note that for any $x \neq x'$,

$$\Pr_{g}\{gx = gx'\} = \frac{1}{|G|}.$$

So the expectation of $l_2$ norm for $g$ satisfy

$$\underset{g}{E}\left[\sum_{h\in G} P_g(h)^2\right] \leqslant \frac{1}{2^l} + \frac{1}{|G|}.$$

Finally, we have the following estimation

$$\begin{aligned}
&\underset{g}{E}\left[\sum_{h\in G}\left|P_g(h) - \frac{1}{|G|}\right|\right] \\
\leqslant &\underset{g}{E}\left[|G|^{\frac{1}{2}}\left(\sum_{h\in G}\left(P_g(h) - \frac{1}{|G|}\right)^2\right)^{\frac{1}{2}}\right] \\
= &|G|^{\frac{1}{2}}\underset{g}{E}\left[\left(\sum_{h\in G} P_g(h)^2 - \frac{1}{|G|}\right)^{\frac{1}{2}}\right] \\
= &|G|^{\frac{1}{2}}\left[\underset{g}{E}\left(\sum_{h\in G} P_g(h)^2\right) - \frac{1}{|G|}\right]^{\frac{1}{2}} \\
\leqslant &(|G|/2^l)^{\frac{1}{2}}.
\end{aligned}$$

We complete the proof. □

The security of LWE public key cryptosystem by Regev is ascribed to the following theorem, which is the most important result in this chapter.

**Theorem 4.2.1** *For any $\epsilon > 0$, $m \geqslant (1+\epsilon)(n+1)logq$, if there is a probabilistic polynomial time algorithm $W$ which distinguishes the plaintext $u = 0$ or $u = 1$ from the ciphertext $c$, then there exists a polynomial time algorithm solving the D-LWE$_{n,q,\chi,m}$ problem.*

***Proof*** The public key of LWE cryptosystem is $A = \begin{pmatrix} \overline{A} \\ b' \end{pmatrix}$, where $\overline{A} \in \mathbb{Z}_q^{n\times m}$ is a matrix uniformly at random, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{Z}_q^m$ is an $m$ dimensional vector chosen uniformly. The encryption function $f_A(u)$ is

$$c = f_A(u) = Ax + \begin{pmatrix} 0 \\ u\lfloor\frac{q}{2}\rceil \end{pmatrix} \in \mathbb{Z}_q^{n+1},\ x \in \{0,1\}^m.$$

Since $W$ is a probabilistic polynomial time algorithm, suppose $P_0(W)$ is the probability that decrypting $u = 0$ from $f_A(0)$ by $W$, and $P_1(W)$ is the probability that decrypting $u = 1$ from $f_A(1)$, i.e.

$$\begin{cases} P_0(W) = Pr\{W(f_A(0)) = 0\}. \\ P_1(W) = Pr\{W(f_A(1)) = 1\}. \end{cases} \tag{4.2.1}$$

If $b \in \mathbb{Z}_q^m$ is uniformly at random, then LWE distribution $A_{s,\chi}$ is uniformly LWE distribution. Let $P_u(W)$ be the probability of decryption successfully by $W$ under the condition of uniformly distribution $A_{s,\chi}$. Suppose that

$$|P_0(W) - P_1(W)| \geqslant \frac{1}{n^\delta},\ \delta > 0. \tag{4.2.2}$$

Under the assumption of (4.2.2), we will construct a new algorithm $W'$ satisfying

$$|P_0(W') - P_u(W')| \geqslant \frac{1}{2n^\delta}. \tag{4.2.3}$$

By (4.2.2), we have

$$|P_0(W) - P_u(W)| \geqslant \frac{1}{2n^\delta},\ \text{or}\ |P_1(W) - P_u(W)| \geqslant \frac{1}{2n^\delta}.$$

If the first inequality of the above formula holds, let $W' = W$. If the second inequality of the above formula holds, then construct $W'$ as follows. Let the function $\sigma$ be $f_A(u) \to f_A(u) + \begin{pmatrix} 0 \\ \frac{q-1}{2} \end{pmatrix}$.

Thus, $\sigma$ maps the LWE distribution $(\overline{A}, b)$ to $(\overline{A}, b + \frac{q-1}{2})$. If $b$ is uniformly at random, so is $b + \frac{q-1}{2}$. We define $W'$ to be the decryption on LWE distribution $(\overline{A}, b + \frac{q-1}{2})$ by $W$. According to (4.1.5),

$$P_0(W) = P_1(W'),\ P_1(W) = P_0(W'),$$

so $W'$ is the algorithm which satisfies (4.2.3).

Let $s \in \mathbb{Z}_q^n$, the public key sample satisfies distribution of $(\overline{A}, b) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m = A_{s,\chi}$. Let $P_0(s)$ be the probability of decryption $u = 0$ successfully by $W'$, i.e.

$$P_0(s) = Pr\{W'(f_A(0)) = 0\}.$$

Similarly, let $P_u(s)$ be the probability of decryption successfully by $W'$ if $(\overline{A}, b)$ is uniformly at random. Suppose

$$|\underset{s}{E}[P_0(s)] - \underset{s}{E}[P_u(s)]| \geqslant \frac{1}{2n^\delta}, \tag{4.2.4}$$

we define

$$Y = \left\{ s \in \mathbb{Z}_q^n \mid |P_0(s) - P_u(s)| \geqslant \frac{1}{4n^\delta} \right\}. \tag{4.2.5}$$

It's easy to prove: if $s \in \mathbb{Z}_q^n$ is uniformly distributed, then we have

$$|Y|/q^n \geqslant \frac{1}{4n^\delta}.$$

Therefore, in order to prove Theorem 4.2.1, we need to find an algorithm $Z$ to determine whether the LWE distribution $A_{s,\chi}$ is uniformly at random for any $s \in Y$. The construction of algorithm $Z$: let $R$ be a probability distribution on $\mathbb{Z}_q^n$ which is uniform LWE distribution or general LWE distribution when $s \in Y$, i.e.

$$R = \text{uniform LWE distribution, or } R = A_{s,\chi},\ s \in Y.$$

Let $\overline{A} = [a_1, \ldots, a_m] \in \mathbb{Z}_q^{n\times m}$, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{Z}_q^m$ be $m$ random samples from distribution $R$. Let $P_0(R)$ be the probability of decryption $u = 0$ successfully by $W'$, where $(a, b) = A_{s,\chi}$, $s \in Y$. In the same way, suppose $P_u(R)$ is the probability of decryption $u = 0$ successfully by $W'$ if $R$ is uniform LWE distribution. We estimate $P_0(R)$ and $P_u(R)$ by using the algorithm $W'$ polynomial times so that the error could be controlled within $\frac{1}{64n^\delta}$. If $|P_0(R) - P_u(R)| \geqslant \frac{1}{16n^\delta}$, then the algorithm $Z$ is effective, otherwise it is noneffective.

We first confirm: if $R$ is uniform LWE distribution, then $Z$ is noneffective with high probability. Because in this case, $(\overline{A}, b) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$, $b$ is uniformly at random. According to Lemma 4.2.1, the Abel group $G = \mathbb{Z}_q^n \times \mathbb{Z}_q$, we have

$$|P_0(R) - P_u(R)| \leqslant 2^{-\Omega(n)},$$

In this case, $Z$ is noneffective.

If $R = A_{s,\chi}$, where $s \in Y$, we are to prove the algorithm $Z$ is effective with probability $\frac{1}{\mathrm{Poly}(n)}$; i.e. one can distinguish $s \in Y$ from uniform distribution. Since $|P_0(R) - P_u(R)| \geqslant \frac{1}{4n^\delta}$, in the average sense we get

$$Pr\left\{ |P_0(R) - P_u(R)| \geqslant \frac{1}{8n^\delta} \right\} \geqslant \frac{1}{8n^\delta}.$$

Thus, the algorithm $Z$ is effective for $A_{s,\chi}$, $s \in Y$ with positive probability. We complete the proof of Theorem 4.2.1. □

## 4.3 Properties of Rounding Function

The public key of LWE cryptosystem by Regev is $A = \begin{pmatrix} \overline{A} \\ b' \end{pmatrix} \in \mathbb{Z}_q^{(n+1)\times m}$, where $\overline{A} \in \mathbb{Z}_q^{n\times m}$ is a matrix uniformly at random, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{Z}_q^m$ is a uniform sample vector (see 4.1.2). In this section we will discuss the sampling technique of public key $A$ based on rounding function.

For $\forall x \in \mathbb{R}$, let $\{x\}$ be the fractional part of $x$, $\lfloor x \rceil$ be the closest integer to $x$, i.e.

$$\lfloor x \rceil = \begin{cases} x - \{x\}, \text{ if } 0 \leqslant \{x\} \leqslant \frac{1}{2}. \\ x + 1 - \{x\}, \text{ if } \frac{1}{2} < \{x\} < 1. \end{cases} \tag{4.3.1}$$

In fact, $\lfloor x \rceil$ is the only integer satisfying

$$x = \lfloor x \rceil + r, \ -\frac{1}{2} < r \leqslant \frac{1}{2}, \text{ if } r = \frac{1}{2} \Leftrightarrow \{x\} = \frac{1}{2}. \tag{4.3.2}$$

We call $\lfloor x \rceil$ rounding function, and its properties could be summarized as the following two lemmas.

**Lemma 4.3.1** *(i)* $\lfloor x + n \rceil = n + \lfloor x \rceil$, $n \in \mathbb{Z}$, $x \in \mathbb{R}$.

*(ii)* $\lfloor -x \rceil = \begin{cases} -\lfloor x \rceil, \ \textit{if } \{x\} \neq \frac{1}{2}. \\ -1 - \lfloor x \rceil, \ \textit{if } \{x\} = \frac{1}{2}. \end{cases}$

*(iii) For any integers $a, b \in \mathbb{Z}$, $b \neq 0$, we have the following division: $a = \lfloor \frac{a}{b} \rceil b + r$, where $-\frac{b}{2} < r \leqslant \frac{b}{2}$.*

*(iv)* $\lfloor x \rceil + \lfloor y \rceil - 1 \leqslant \lfloor x + y \rceil \leqslant \lfloor x \rceil + \lfloor y \rceil + 1$, $\forall x, y \in \mathbb{R}$.

*(v)* $\lfloor \frac{\lfloor x \rceil}{n} \rceil = \lfloor \frac{x}{n} \rceil$, $\forall n \in \mathbb{Z}$, $n \geqslant 1$, $x \in \mathbb{R}$.

***Proof*** By (4.3.2),

$$\lfloor x + n \rceil = \lfloor \lfloor x \rceil + r + n \rceil = n + \lfloor x \rceil,$$

so (i) holds. If $\{x\} \neq \frac{1}{2}$, then $r \neq \frac{1}{2}$, and $-\frac{1}{2} < r < \frac{1}{2}$, we have

$$\lfloor -x \rceil = \lfloor -\lfloor x \rceil - r \rceil = -\lfloor x \rceil.$$

If $r = \frac{1}{2}$, then $\{x\} = \frac{1}{2}$, and $1 - r = \frac{1}{2}$, so that

$$\lfloor -x \rceil = \lfloor -\lfloor x \rceil - 1 + 1 - r \rceil = -1 - \lfloor x \rceil,$$

we have (ii). Property (iii) and (iv) can be proved similarly. To prove (v), let $x = \lfloor x \rceil + r$, then $-\frac{1}{2n} < \frac{r}{n} \leqslant \frac{1}{2n}$, thus,

$$\lfloor \frac{x}{n} \rceil = \lfloor \frac{\lfloor x \rceil}{n} + \frac{r}{n} \rceil = \frac{\lfloor x \rceil}{n}.$$

Lemma 4.3.1 holds. □

**Definition 4.3.1** Let $t$ and $q$ be two positive integers, we define function $f : \mathbb{Z} \to \mathbb{Z}$ as

$$f(a) = \lfloor \frac{q}{t} a \rceil, \ \forall a \in \mathbb{Z}. \tag{4.3.3}$$

**Lemma 4.3.2** *Let $a, b \in \mathbb{Z}$, then*

$$a \equiv b \ (mod\ t) \Rightarrow f(a) \equiv f(b) \ (mod\ q).$$

***Proof*** Since $a \equiv b \pmod{t}$, we write $a = st + b$, therefore

$$f(a) = \lfloor \frac{q}{t}(st + b) \rceil = \lfloor sq + \frac{q}{t} b \rceil = sq + \lfloor \frac{q}{t} b \rceil = sq + f(b).$$

So we have $f(a) \equiv f(b) \pmod{q}$. □

By the above lemma, $f$ is a function from $\mathbb{Z}_t$ to $\mathbb{Z}_q$, we can define its 'inverse function' $f^{-1} : \mathbb{Z}_q \to \mathbb{Z}_t$ as follows

$$f^{-1}(b) = \lfloor \frac{tb}{q} \rceil, \ \forall b \in \mathbb{Z}_q. \tag{4.3.4}$$

**Lemma 4.3.3** *(i) If $t \leqslant q$, then $\forall a \in \mathbb{Z}$, we have*

$$f^{-1} f(a) = a.$$

*(ii) If $t > q$, and $a \in \mathbb{Z}$ is uniformly chosen at random, we have*

$$Pr\{f^{-1} f(a) \neq a\} = 1 - \frac{q}{t}. \tag{4.3.5}$$

***Proof*** We first prove (i). If $t = q$, then

$$f(a) = \lfloor \frac{q}{t} a \rceil = \lfloor a \rceil = a \Rightarrow f^{-1} f(a) = f^{-1}(a) = \lfloor \frac{t}{q} a \rceil = \lfloor a \rceil = a, \ \forall a \in \mathbb{Z}.$$

If $t < q$, then $\frac{q}{2t} > \frac{1}{2}$, based on the definition of rounding function,

$$\frac{q}{t} a - \frac{1}{2} \leqslant \lfloor \frac{q}{t} a \rceil < \frac{q}{t} a + \frac{1}{2},$$

it follows that

$$\frac{q}{t}a - \frac{q}{2t} < \frac{q}{t}a - \frac{1}{2} \leqslant \lfloor \frac{q}{t}a \rceil < \frac{q}{t}a + \frac{1}{2} < \frac{q}{t}a + \frac{q}{2t}.$$

So we can get

$$\frac{q}{t}a - \frac{q}{2t} < \lfloor \frac{q}{t}a \rceil < \frac{q}{t}a + \frac{q}{2t},$$

this is equivalent to

$$a - \frac{1}{2} < \frac{t}{q}\lfloor \frac{q}{t}a \rceil < a + \frac{1}{2},$$

$$-\frac{1}{2} < \frac{t}{q}\lfloor \frac{q}{t}a \rceil - a < \frac{1}{2}.$$

Thus,

$$\lfloor \frac{t}{q}\lfloor \frac{q}{t}a \rceil - a \rceil = 0 \Rightarrow \lfloor \frac{t}{q}\lfloor \frac{q}{t}a \rceil \rceil = a.$$

This means that

$$f^{-1}f(a) = a, \ \forall a \in \mathbb{Z}.$$

Next we prove (ii), at this time $q < t$. By Lemma 4.3.2, we only need to consider how many elements $a$ in $\mathbb{Z}_t$ that satisfies $f^{-1}f(a) \neq a$. By (i) we get

$$\lfloor \frac{q}{t}\lfloor \frac{t}{q}b \rceil \rceil = b, \ \forall b \in \mathbb{Z}_q.$$

This is equivalent to

$$f\left(\lfloor \frac{t}{q}b \rceil\right) = b, \ \forall b \in \mathbb{Z}_q.$$

So we have

$$f^{-1}f\left(\lfloor \frac{t}{q}b \rceil\right) = f^{-1}(b) = \lfloor \frac{t}{q}b \rceil, \ \forall b \in \mathbb{Z}_q.$$

Here $0, \left\lfloor \frac{t}{q} \right\rceil, \left\lfloor \frac{2t}{q} \right\rceil, \ldots, \left\lfloor \frac{(q-1)t}{q} \right\rceil$ are different from each other in $\mathbb{Z}_t$. Next we prove that the number of $a$ in $\mathbb{Z}_t$ satisfying $f^{-1}(f(a)) = a$ is no more than $q$. Let $A$ be the set containing all the elements satisfying $f^{-1}(f(a)) = a$ in $\mathbb{Z}_t$. $\forall a_1, a_2 \in A, a_1 \neq a_2$ in $\mathbb{Z}_t$, then we have $f(a_1) \not\equiv f(a_2) \pmod{q}$, i.e. $f(a_1) \neq f(a_2)$ in $\mathbb{Z}_q$. This means the number of $A$ is no more than $q$. Above all, it shows that $0, \left\lfloor \frac{t}{q} \right\rceil, \left\lfloor \frac{2t}{q} \right\rceil, \ldots, \left\lfloor \frac{(q-1)t}{q} \right\rceil$ are just all the numbers in $\mathbb{Z}_t$ such that $f^{-1}(f(a)) = a$. Based on $a$ is uniformly chosen in $\mathbb{Z}_t$, then

$$Pr\{f^{-1}f(a) \neq a\} = 1 - \frac{q}{t}.$$

We complete the proof. □

In order to generalize the function $f$ and $f^{-1}$ from one dimension to high dimension, we give the following definition.

**Definition 4.3.2** Let $t, q, l$ be positive integers, we define function $F : \mathbb{Z}_t^l \to \mathbb{Z}_q^l$ as

$$F(a) = \left(\lfloor \frac{q}{t}a_1 \rceil, \lfloor \frac{q}{t}a_2 \rceil, \ldots, \lfloor \frac{q}{t}a_l \rceil\right) \in \mathbb{Z}_q^l,\ \forall a = (a_1, a_2, \ldots, a_l) \in \mathbb{Z}_t^l, \quad (4.3.6)$$

and the 'inverse function' $F^{-1} : \mathbb{Z}_q^l \to \mathbb{Z}_t^l$ as

$$F^{-1}(b) = \left(\lfloor \frac{t}{q}b_1 \rceil, \lfloor \frac{t}{q}b_2 \rceil, \ldots, \lfloor \frac{t}{q}b_l \rceil\right) \in \mathbb{Z}_t^l,\ \forall b = (b_1, b_2, \ldots, b_l) \in \mathbb{Z}_q^l. \quad (4.3.7)$$

**Lemma 4.3.4** *$\forall a = (a_1, a_2, \ldots, a_l) \in \mathbb{Z}_t^l$, if $a$ is uniformly at random and $a_1, a_2, \ldots, a_l$ are mutually independent, we have*

$$Pr\{F^{-1}F(a) \neq a\} = \max\left\{0, 1 - \left(\frac{q}{t}\right)^l\right\}. \quad (4.3.8)$$

***Proof*** If $t \leqslant q$, from Lemma 4.3.3,

$$f^{-1}f(a_i) = a_i,\ \forall a_i \in \mathbb{Z}_t,\ \forall 1 \leqslant i \leqslant l.$$

So

$$F^{-1}F(a) = a,\ \forall a \in \mathbb{Z}_t^l.$$

$$Pr\{F^{-1}F(a) \neq a\} = 0 = \max\left\{0, 1 - \left(\frac{q}{t}\right)^l\right\}.$$

If $t > q$, from Lemma 4.3.3,

$$Pr\{f^{-1}f(a_i) = a_i\} = \frac{q}{t},\ a_i \in \mathbb{Z}_t,\ \forall 1 \leqslant i \leqslant l.$$

Since $a_1, a_2, \ldots, a_l$ are independent, therefore,

$$Pr\{F^{-1}F(a) = a\} = \left(\frac{q}{t}\right)^l,\ a \in \mathbb{Z}_t^l.$$

$$Pr\{F^{-1}F(a) \neq a\} = 1 - \left(\frac{q}{t}\right)^l = \max\{0, 1 - (\frac{q}{t})^l\}.$$

We finish the proof. □

## 4.4 General LWE-Based Cryptosystem

We introduced the LWE cryptosystem proposed by Regev in Sect. 4.1 and proved its security in Sect. 4.2. However, it could only encrypt a single bit of plaintext and the efficiency is low. Based on the definition and properties of rounding function given in Sect. 4.3, Regev presented a general LWE cryptosystem in 2009 Regev (2010), which could encrypt multiple bits of plaintext $v \in \mathbb{Z}_t^l$ with size $O(t^l)$ and improve the efficiency signally. In this section, we introduce general LWE cryptosystem first. Then we discuss the probability of decryption error for this cryptosystem and prove that it could be sufficiently small with suitable parameters. So we verify our core result that the LWE cryptosystem could have high security.

Let $t, q, m, n, l, r$ be positive integers, $q > t$, function $F$ and its 'inverse function' are defined in 3.2. The workflow of general LWE cryptosystem is as follows:

(1) Selection of private key $S$: $S \in \mathbb{Z}_q^{n\times l}$ is an $n \times l$ matrix uniformly at random in $\mathbb{Z}_q$.

In the LWE cryptosystem introduced in Sect. 4.1, the private key is an $n$ dimensional randomly chosen vector $s \in \mathbb{Z}_q^n$. To encrypt more general plaintext $v \in \mathbb{Z}_t^l$, we randomly select $l$ private keys $s_1, s_2, \ldots, s_l \in \mathbb{Z}_q^n$ independently and form an $n \times l$ matrix $S = [s_1, s_2, \ldots, s_l]$. This is the private key $S$ for general LWE cryptosystem.

(2) Public key.
When the private key $S \in \mathbb{Z}_q^{n\times l}$ is fixed, in order to choose samples from LWE distribution, we first select $m$ uniform $n$ dimensional vectors $a_1, a_2, \ldots, a_m \in \mathbb{Z}_q^n$ in $\mathbb{Z}_q^n$ and form a uniform random matrix

$$A = [a_1, a_2, \ldots, a_m]_{n\times m} \in \mathbb{Z}_q^{n\times m}.$$

Then we generate $m \times l$ noise matrix samples $E = (E_{ij})_{m\times l}$ from distribution $\overline{\psi}_\alpha$, where $\overline{\psi}_\alpha$ is defined by (4.4.1) and (3.3.13), i.e. $E_{ij} \in \mathbb{Z}_q$, $E_{ij} \leftarrow \overline{\psi}_\alpha$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant l$, and the $m \times l$ samples are mutually independent. Finally we get an $m \times l$ matrix $P$

$$P = A^T S + E = \begin{pmatrix} < a_1, s_1 > +E_{11} & \cdots & < a_1, s_l > +E_{1l} \\ \vdots & \ddots & \vdots \\ < a_m, s_1 > +E_{m1} & \cdots & < a_m, s_l > +E_{ml} \end{pmatrix}_{m\times l}.$$

The public key of LWE cryptosystem is $(A, P)$, which is similar to that in Sect. 4.1. Here we only change the public key from $b \in \mathbb{Z}_q^m$ to $m \times l$ matrix $P \in \mathbb{Z}_q^{m\times l}$. If the uniformly random matrix $A$ is given and saved for all the users of LWE cryptosystem, then the true public key is the matrix $P$, and the public key and private key satisfy the following equation

$$P - A^T S \equiv_{\overline{\psi}_\alpha} E \pmod q.$$

(3) Encryption.

To encrypt multiple bits of plaintext $v \in \mathbb{Z}_t^l$, let $a \in \{-r, -r+1, \ldots, r\}^m$ be an $m$ dimensional vector with each entry selected uniformly in $\{-r, -r+1, \ldots, r\}$, i.e. $a$ is uniformly distributed. Ciphertext $\begin{pmatrix} u \\ c \end{pmatrix}$ is an $n + l$ dimensional vector, defined by

$$g_{A,P}(v) = \begin{pmatrix} u \\ c \end{pmatrix}, \ u = Aa, \ c = P^T a + F(v),$$

where $F$ is defined in (4.3.6), and $g_{A,P}$ is called the encryption algorithm of LWE cryptosystem.

(4) Decryption.
Given ciphertext $(u, c)$ and the private key $S$, we compute $F^{-1}(c - S^T u)$ as the result of decryption. We have

$$\begin{aligned} F^{-1}(c - S^T u) &= F^{-1}(P^T a + F(v) - S^T u) \\ &= F^{-1}((A^T S + E)^T a + F(v) - S^T A a) \\ &= F^{-1}(E^T a + F(v)). \end{aligned}$$

Next we calculate the probability of decryption error for this cryptosystem, namely the probability of $F^{-1}(E^T a + F(v)) \neq v$. The following Theorem 4.4.1 gives an estimation for this probability, which is the main result of this section.

**Theorem 4.4.1** *Suppose $q > t$, we have the following inequality of the probability of decryption error*

$$Pr\{F^{-1}(E^T a + F(v)) \neq v\} \leqslant 2l\Big(1 - \Phi\Big(\frac{q-t}{2\alpha t q}\sqrt{\frac{6\pi}{mr(r+1)}}\Big)\Big). \tag{4.4.1}$$

*Here $\Phi$ is the cumulative distribution function of the standard normal distribution, i.e. $\Phi(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} \mathrm{d}t$.*

***Proof*** Denote $v=(v_1, v_2, \ldots, v_l)$, $E_{m\times l} = (E_1, E_2, \ldots, E_l)$, where $E_1, E_2, \ldots, E_l$ are all $m$ dimensional column vectors. Let $f^{-1}(E_i^T a + f(v_i))$ be the $i$th coordinate of $F^{-1}(E^T a + F(v))$, $1 \leqslant i \leqslant l$. According to the definition of rounding function,

$$-\frac{1}{2} < \frac{q}{t}v_i - \lfloor \frac{q}{t}v_i \rceil \leqslant \frac{1}{2},$$

$$-\frac{t}{2q} \leqslant \frac{t}{q}\lfloor \frac{q}{t}v_i \rceil - v_i < \frac{t}{2q}.$$

So if $\left|\frac{t}{q}E_i^T a\right| < \frac{1}{2} - \frac{t}{2q}$, we get

$$\left|\frac{t}{q}E_i^T a + \frac{t}{q}\lfloor \frac{q}{t}v_i \rceil - v_i\right| < \frac{1}{2} - \frac{t}{2q} + \frac{t}{2q} = \frac{1}{2}.$$

It follows that

$$\lfloor \frac{t}{q}E_i^T a + \frac{t}{q}\lfloor \frac{q}{t}v_i \rceil - v_i \rceil = 0,$$

this means

$$\lfloor \frac{t}{q}E_i^T a + \frac{t}{q}\lfloor \frac{q}{t}v_i \rceil \rceil = v_i,$$

$$f^{-1}\left(E_i^T a + f(v_i)\right) = v_i.$$

namely if $|\frac{t}{q}E_i^T a| < \frac{1}{2} - \frac{t}{2q}$, we can get $f^{-1}(E_i^T a + f(v_i)) = v_i$. Equivalently, if $f^{-1}\left(E_i^T a + f(v_i)\right) \neq v_i$, i.e. the decryption error occurs in the $i$th letter, then $\left|\frac{t}{q}E_i^T a\right| \geqslant \frac{1}{2} - \frac{t}{2q}$. So the probability of decryption error in one letter is no more than the probability of $\left|\frac{t}{q}E_i^T a\right| \geqslant \frac{1}{2} - \frac{t}{2q}$, i.e.

$$Pr\left\{f^{-1}\left(E_i^T a + f(v_i)\right) \neq v_i\right\} \leqslant Pr\left\{\left|\frac{t}{q}E_i^T a\right| \geqslant \frac{1}{2} - \frac{t}{2q}\right\}.$$

The next step we estimate the probability of $|\frac{t}{q}E_i^T a| \geqslant \frac{1}{2} - \frac{t}{2q}$. Since each coordinate of $E_i$ is chosen independently from the Gaussian distribution with mean 0 and standard deviation $\alpha q/\sqrt{2\pi}$ and the sum of independent Gaussian variables is still a Gaussian variable, $E_i^T a$ is also a Gaussian distribution variable. Let $a = (a_1, a_2, \ldots, a_m)$ and each $a_i$ is chosen from $\{-r, -r+1, \cdots, r\}$ uniformly at random, then

$$E(a_i) = \frac{-r + (-r+1) + \cdots + r}{2r+1} = 0,$$

$$Var(a_i) = \frac{(-r)^2 + (-r+1)^2 + \cdots + r^2}{2r+1} = \frac{r(r+1)}{3}.$$

$$E(E_i^T a) = 0.$$

$$Var\left(E_i^T a\right) = \left(\frac{\alpha q}{\sqrt{2\pi}}\right)^2 \cdot \frac{r(r+1)}{3} m = \frac{\alpha^2 q^2\, mr(r+1)}{6\pi}.$$

Therefore $E_i^T a$ is treated as a normal distribution with mean 0 and standard deviation $\alpha q\sqrt{mr(r+1)}/\sqrt{6\pi}$. We have

$$Pr\left\{\left|\frac{t}{q}E_i^T a\right| \geqslant \frac{1}{2} - \frac{t}{2q}\right\} = P\left\{\left|E_i^T a\right| \geqslant \frac{q-t}{2t}\right\}$$

$$= Pr\left\{\left|E_i^T a\right| / \left(\alpha q\sqrt{\frac{mr(r+1)}{6\pi}}\right) \geqslant \frac{q-t}{2t} / (\alpha q\sqrt{\frac{mr(r+1)}{6\pi}})\right\}$$

$$= Pr\left\{\left|E_i^T a\right| / \left(\alpha q\sqrt{\frac{mr(r+1)}{6\pi}}\right) \geqslant \frac{q-t}{2\alpha tq}\sqrt{\frac{6\pi}{mr(r+1)}}\right\}$$

$$= 2\Big(1 - \Phi\big(\frac{q-t}{2\alpha tq}\sqrt{\frac{6\pi}{mr(r+1)}}\big)\Big).$$

So we get the following inequality for probability of decryption error of the LWE cryptosystem

$$Pr\{F^{-1}(E^T a + F(v)) \neq v\}$$

$$\leqslant lPr\left\{f^{-1}\left(E_i^T a + f(v_i)\right) \neq v_i\right\}$$

$$\leqslant lPr\left\{\left|\frac{t}{q}E_i^T a\right| \geqslant \frac{1}{2} - \frac{t}{2q}\right\}$$

$$= 2l\Big(1 - \Phi\big(\frac{q-t}{2\alpha tq}\sqrt{\frac{6\pi}{mr(r+1)}}\big)\Big).$$

□

The upper bound could be as closed as 0 if we choose $\alpha$ small enough. It means that the probability of decryption error for the LWE cryptosystem could be made very small with an appropriate setting of parameters.

## 4.5 Probability of Decryption Error for General Disturbance

In this section we estimate the probability of decryption error for the LWE cryptosystem when the noise matrix $E = (E_{ij})_{m\times l}$ is chosen independently from a general common variable, rather than Gauss distribution. We have the following theorem.

**Theorem 4.5.1** *$q > t$, $E = (E_{ij})_{m\times l}$, each element $E_{ij}$ is selected independently from a common random variable of mean 0 and standard deviation $\beta$. For any $\delta > 0$, we can find positive integer $m$, such that the following inequality of the probability of decryption error holds,*

$$Pr\{F^{-1}(E^T a + F(v)) \neq v\} \leqslant 2l\Big(1 - \Phi\big(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr(r+1)}}\big)\Big) + l\delta, \quad (4.5.1)$$

*Here $\Phi$ is the cumulative distribution function of the standard normal distribution, i.e. $\Phi(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} \mathrm{d}t$.*

***Proof*** Similarly as the proof of Theorem 4.4.1, we need to estimate the probability of $|\frac{t}{q}E_i^T a| \geqslant \frac{1}{2} - \frac{t}{2q}$. Since the coordinates of $E_i^T$ are independent identically distributed, $E_i^T$ and $a$ are also independent. By central limit theorem Riauba (1975), $E_i^T a$ is approximately normal distribution with mean 0 and standard deviation $d = \sqrt{mVar(E_{ij})Var(a_i)} = \beta\sqrt{\frac{mr(r+1)}{3}}$. Thus, for any sufficiently small $\delta > 0$, there is a positive integer $m$ such that

$$P\left\{\left|\frac{t}{q}E_i^T a\right| \geqslant \frac{1}{2} - \frac{t}{2q}\right\} = P\left\{\left|E_i^T a\right| \geqslant \frac{q-t}{2t}\right\}$$

$$= P\left\{\left|E_i^T a\right| / \left(\beta\sqrt{\frac{mr(r+1)}{3}}\right) \geqslant \frac{q-t}{2t} / \left(\beta\sqrt{\frac{mr(r+1)}{3}}\right)\right\}$$

$$= P\left\{\left|E_i^T a\right| / \left(\beta\sqrt{\frac{mr(r+1)}{3}}\right) \geqslant \frac{q-t}{2\beta t}\sqrt{\frac{3}{mr(r+1)}}\right\}$$

$$= 2\Big(1 - \Phi\big(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr(r+1)}}\big)\Big) + \varepsilon,$$

Here $|\varepsilon| \leqslant \delta$. Then we get the following inequality for probability of decryption error of the LWE cryptosystem for general disturbance

$$Pr\{F^{-1}(E^T a + F(v)) \neq v\}$$

$$\leqslant lPr\left\{f^{-1}\left(E_i^T a + f(v_i)\right) \neq v_i\right\}$$

$$\leqslant lPr\left\{\left|\frac{t}{q}E_i^T a\right| \geqslant \frac{1}{2} - \frac{t}{2q}\right\}$$

$$= 2l\Big(1 - \Phi\big(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr(r+1)}}\big)\Big) + l\varepsilon.$$

$$\leqslant 2l\Big(1 - \Phi\big(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr(r+1)}}\big)\Big) + l\delta.$$

□

This probability could be also closed to 0 if we choose the parameter $\beta\sqrt{m}$ and $\delta$ small enough. Therefore the probability of decryption error of the LWE cryptosystem for general disturbance could be made very small, which leads to high security.

**Example 4.5.1** Let $t = 2, q = 5, l = 1, m = 1, r = 1, \delta = 10^{-3}, \beta = 10^{-3}, v \in \mathbb{Z}_2$ is uniformly chosen at random, the disturbance $E$ is a random variable with the distribution $\psi_\beta$ such that $P\{E = k\} = \frac{\beta^k}{2\cdot k!}e^{-\beta}$ for positive integer $k$ and $Pr\{E = 0\} = e^{-\beta}$, $a \in \{-1, 0, 1\}$ is uniformly chosen at random. Then the probability of decryption error

$$Pr\{F^{-1}(Ea + F(v)) \neq v\} = Pr\left\{\lfloor\frac{2}{5}\left(Ea + \lfloor\frac{5}{2}v\rceil\right)\rceil \neq v\right\}$$

$$= \frac{1}{2}Pr\left\{\lfloor\frac{2}{5}Ea\rceil \neq 0\right\} + \frac{1}{2}Pr\left\{\lfloor\frac{2}{5}(Ea+2)\rceil \neq 1\right\}$$

$$\leqslant \frac{1}{2}Pr\{E \neq 0\} + \frac{1}{2}Pr\{E \neq 0\}$$

$$= 1 - Pr\{E = 0\} = 1 - e^{-0.001} < 10^{-3}.$$

On the other hand,

$$2l\Big(1 - \Phi\big(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr(r+1)}}\big)\Big) + l\delta > 10^{-3}.$$

So it follows that

$$Pr\{F^{-1}(Ea + F(v)) \neq v\} < 2l\Big(1 - \Phi\big(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr(r+1)}}\big)\Big) + l\delta,$$

The inequality in Theorem 4.5.1 holds.

**Example 4.5.2** Let $t = 2, q = 5, l = 1, m = 1, r = 1, \delta = 10^{-4}, \lambda = 0.05, v \in \mathbb{Z}_2$ is uniformly chosen at random, the disturbance $E$ is a Laplace distribution variable with probability density function $f(x) = \frac{1}{2\lambda}e^{-\frac{|x|}{\lambda}}$ rounding to the nearest integer, $a \in \{-1, 0, 1\}$ is uniformly chosen at random. Similarly as Example 4.5.1, the probability of decryption error

$$Pr\{F^{-1}(Ea + F(v)) \neq v\} = Pr\left\{\lfloor\frac{2}{5}\left(Ea + \lfloor\frac{5}{2}v\rceil\right)\rceil \neq v\right\}$$

$$\leqslant 1 - Pr\{E = 0\} = 1 - \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{1}{2\lambda} e^{-\frac{|x|}{\lambda}} \mathrm{d}x = e^{-10} < 10^{-4}.$$

On the other hand,

$$2l\Big(1 - \Phi\big(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr(r+1)}}\big)\Big) + l\delta > 10^{-4}.$$

We have

$$Pr\{F^{-1}(Ea + F(v)) \neq v\} < 2l\Big(1 - \Phi\big(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr(r+1)}}\big)\Big) + l\delta,$$

The inequality in Theorem 4.5.1 holds.



# Chapter 5
# Cyclic Lattices and Ideal Lattices


Cyclic lattices and ideal lattices were introduced by Micciancio (2002), Lyubashevsky and Micciancio (2006), respectively, which play an efficient role in Ajtai's construction of a collision-resistant Hash function and in Gentry's construction of fully homomorphic encryption (Gentry, 2009a). Let $R = \mathbb{Z}[x]/ < \phi(x) >$ be a quotient ring of the integer coefficients polynomials ring, Lyubashevsky and Micciancio regarded an ideal lattice as the correspondence of an ideal of $R$, but they neither explain how to extend this definition to whole Euclidean space $\mathbb{R}^n$, nor exhibit the relationship of cyclic lattices and ideal lattices. In this chapter, we regard the cyclic lattices and ideal lattices as the correspondences of finitely generated $R$-modules, so that we may show that ideal lattices are actually a special subclass of cyclic lattices, namely cyclic integer lattices. It is worth noting that we use more general rotation matrix here, so our definition and results on cyclic lattices and ideal lattices are more general forms. As application, we provide cyclic lattice with an explicit and countable upper bound for the smoothing parameter. Our results may be viewed as a substantial progress in this direction.

## 5.1 Some Basic Properties of Lattice

At the beginning of Chap. 1, we have introduced the definition of lattice in $\mathbb{R}^n$. A lattice is actually a discrete additive subgroup. In this section, we mainly give some properties of lattice that will be used later in this chapter.

**Lemma 5.1.1** *Let $L \subset \mathbb{R}^n$ be a lattice, $\alpha_1, \alpha_2, \ldots, \alpha_m \in L$ be $m$ vectors of $L$. Then $\alpha_1, \alpha_2, \ldots, \alpha_m$ are linearly independent over $\mathbb{R}$, if and only if they are linearly independent over $\mathbb{Z}$.*

***Proof*** If $\alpha_1, \alpha_2, \ldots, \alpha_m$ are linearly independent over $\mathbb{R}$, trivially which are linearly independent over $\mathbb{Z}$. Suppose that $\alpha_1, \alpha_2, \ldots, \alpha_m$ are linearly independent over $\mathbb{Z}$, we consider arbitrary linear combination over $\mathbb{R}$. Let

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m = 0, \tag{5.1.1}$$



Z. Zheng et al., *Modern Cryptography Volume 2*, Financial Mathematics and Fintech,
https://doi.org/10.1007/978-981-19-7644-5_5

We should prove (5.1.1) is equivalent to $a_1 = a_2 = \cdots = a_m = 0$, which implies that $\alpha_1, \alpha_2, \ldots, \alpha_m$ are linearly independent over $\mathbb{R}$.

By Minkowski's Third theorem (see theorem VII of Cassels (1963)), for any sufficiently large $N > 1$, there are a positive integer $q \geqslant 1$ and integers $p_1, p_2, \ldots, p_m \in \mathbb{Z}$ such that

$$\max_{1 \leqslant i \leqslant m} |qa_i - p_i| < N^{-\frac{1}{m}}, \ 1 \leqslant q \leqslant N. \tag{5.1.2}$$

By (5.1.1), we have

$$\begin{aligned} &|p_1\alpha_1 + p_2\alpha_2 + \cdots + p_m\alpha_m| \\ &\quad = |(qa_1 - p_1)\alpha_1 + (qa_2 - p_2)\alpha_2 + \cdots + (qa_m - p_m)\alpha_m| \\ &\quad \leqslant mN^{-\frac{1}{m}} \max_{1 \leqslant i \leqslant m} |\alpha_i|. \end{aligned} \tag{5.1.3}$$

Let $\lambda$ be the minimum distance of $L$, $\epsilon > 0$ be any positive real number. We select $N$ such that

$$N > \max\left\{\left(\frac{m}{\epsilon}\right)^m, \left(\frac{m}{\lambda}\right)^m \max_{1 \leqslant i \leqslant m} |\alpha_i|^m\right\},$$

It follows that $mN^{-\frac{1}{m}} < \epsilon$ and

$$mN^{-\frac{1}{m}} \max_{1 \leqslant i \leqslant m} |\alpha_i| < \lambda.$$

By (5.1.3) we have

$$|p_1\alpha_1 + p_2\alpha_2 + \cdots + p_m\alpha_m| < \lambda.$$

Since $p_1\alpha_1 + p_2\alpha_2 + \cdots + p_m\alpha_m \in L$, thus we have $p_1\alpha_1 + p_2\alpha_2 + \cdots + p_m\alpha_m = 0$, and $p_1 = p_2 = \cdots = p_m = 0$. By (5.1.2) we have $q|a_i| < \frac{1}{m}\varepsilon$ for all $i$, $1 \leqslant i \leqslant m$. Since $\varepsilon$ is sufficiently small positive number, we must have $a_1 = a_2 = \cdots = a_m = 0$. We complete the proof of lemma. □

Suppose that $B \in \mathbb{R}^{n \times m}$ is an $n \times m$ dimensional matrix and $\text{rank}(B) = m$, $B^T$ is the transpose of $B$. It is easy to verify

$$\text{rank}(B^T B) = \text{rank}(B) = m \Rightarrow \det(B^T B) \neq 0,$$

which implies that $B^T B$ is an invertible square matrix of $m \times m$ dimension. Since $B^T B$ is a positive defined symmetric matrix, then there is an orthogonal matrix $P \in \mathbb{R}^{m \times m}$ such that

$$P^T B^T B P = \text{diag}\{\delta_1, \delta_2, \ldots, \delta_m\}, \tag{5.1.4}$$

where $\delta_i > 0$ are the characteristic value of $B^T B$, and $\text{diag}\{\delta_1, \delta_2, \ldots, \delta_m\}$ is the diagonal matrix of $m \times m$ dimension.

**Lemma 5.1.2** *Suppose that $B \in \mathbb{R}^{n\times m}$ with rank$(B) = m$, $\delta_1, \delta_2, \ldots, \delta_m$ are $m$ characteristic values of $B^T B$, and $\lambda(L(B))$ is the minimum distance of lattice $L(B)$, then we have*

$$\lambda(L(B)) = \min_{x\in\mathbb{Z}^m,\ x\neq 0} |Bx| \geqslant \sqrt{\delta}, \tag{5.1.5}$$

*where $\delta = \min\{\delta_1, \delta_2, \ldots, \delta_m\}$.*

***Proof*** Let $A = B^T B$, by (5.1.4), there exists an orthogonal matrix $P \in \mathbb{R}^{m\times m}$ such that

$$P^T AP = \text{diag}\{\delta_1, \delta_2, \ldots, \delta_m\}.$$

If $x \in \mathbb{Z}^m$, $x \neq 0$, we have

$$\begin{aligned} |Bx|^2 &= x^T Ax = x^T P(P^T AP)P^T x \\ &= (P^T x)^T \text{ diag}\{\delta_1, \delta_2, \ldots, \delta_m\}P^T x \\ &\geqslant \delta|P^T x|^2 = \delta|x|^2. \end{aligned}$$

Since $x \in \mathbb{Z}^m$ and $x \neq 0$, we have $|x|^2 \geqslant 1$, it follows that

$$\min_{x\in\mathbb{Z}^m,\ x\neq 0} |Bx| \geqslant \sqrt{\delta}|x| \geqslant \sqrt{\delta}.$$

We have lemma 5.1.2 immediately. □

Another application of lemma 5.1.2 is to give a countable upper bound for smoothing parameters in Sect. 5.4. A sublattice $N$ of $L$ means a discrete additive subgroup of $L$, the quotient group is written by $L/N$ and the cardinality of $L/N$ is denoted by $|L/N|$.

**Lemma 5.1.3** *Let $L \subset \mathbb{R}^n$ be a lattice and $N \subset L$ be a sublattice. If rank$(N)$ =rank $(L)$, then the quotient group $L/N$ is a finite group.*

***Proof*** Let rank$(L) = m$, and $L = L(B)$, where $B \in \mathbb{R}^{n\times m}$ with rank$(B) = m$. We define a mapping $\sigma$ from $L$ to $\mathbb{Z}^m$ by $\sigma(Bx) = x$. Clearly, $\sigma$ is an additive group isomorphism, $\sigma(N) \subset \mathbb{Z}^m$ is a full-rank lattice of $\mathbb{Z}^m$, and $L/N \cong \mathbb{Z}^m/\sigma(N)$. It is a well-known result that

$$|\mathbb{Z}^m/\sigma(N)| = \det(\sigma(N)),$$

It follows that

$$|L/N| = |\mathbb{Z}^m/\sigma(N)| = \det(\sigma(N)).$$

Lemma 5.1.3 follows. □

Suppose that $L_1 \subset \mathbb{R}^n, L_2 \subset \mathbb{R}^n$ are two lattices of $\mathbb{R}^n$, we define $L_1 + L_2 = \{a + b | a \in L_1, b \in L_2\}$. Obviously, $L_1 + L_2$ is an additive subgroup of $\mathbb{R}^n$, but generally speaking, $L_1 + L_2$ is not a lattice of $\mathbb{R}^n$ again.

**Lemma 5.1.4** *Let $L_1 \subset \mathbb{R}^n$, $L_2 \subset \mathbb{R}^n$ be two lattices of $\mathbb{R}^n$. If rank$(L_1 \cap L_2)$ =rank $(L_1)$ or rank$(L_1 \cap L_2)$ =rank$(L_2)$, then $L_1 + L_2$ is again a lattice of $\mathbb{R}^n$.*

***Proof*** To prove $L_1 + L_2$ is a lattice of $\mathbb{R}^n$, it is sufficient to prove $L_1 + L_2$ is a discrete subgroup of $\mathbb{R}^n$. Suppose that rank$(L_1 \cap L_2)$ =rank$(L_1)$, for any $x \in L_1$, we define a distance function $\rho(x)$ by

$$\rho(x) = \inf\{|x - y| \Big| y \neq x, \ y \in L_2\}.$$

Since there are only finitely many vectors in $L_2 \cap N(x, \delta)$, where $N(x, \delta)$ is any a ball of center $x$ with radius $\delta$. Therefore, we have

$$\rho(x) = \min\{|x - y| \Big| y \neq x, \ y \in L_2\} = \lambda_x > 0. \tag{5.1.6}$$

On the other hand, if $x_1 \in L_1, x_2 \in L_1$ and $x_1 - x_2 \in L_2$, then there is $y_0 \in L_2$ such that $x_1 = x_2 + y_0$, and we have $\rho(x_1) = \rho(x_2)$. It means that $\rho(x)$ is defined over the quotient group $L_1 + L_2/L_2$. Because we have the following group isomorphic theorem

$$L_1 + L_2/L_2 \cong L_1/L_1 \cap L_2,$$

By lemma 5.1.3, it follows that

$$|L_1 + L_2/L_2| = |L_1/L_1 \cap L_2| < \infty,$$

In other words, $L_1 + L_2/L_2$ is also a finite group. Let $x_1, x_2, \ldots, x_k$ be the representative elements of $L_1 + L_2/L_2$, we have

$$\min_{x \in L_1, y \in L_2, x \neq y} |x - y| = \min_{1 \leqslant i \leqslant k} \rho(x_i) \geqslant \min\{\lambda_{x_1}, \lambda_{x_2}, \ldots, \lambda_{x_k}\} > 0.$$

Therefore, $L_1 + L_2$ is a discrete subgroup of $\mathbb{R}^n$, thus it is a lattice of $\mathbb{R}^n$. □

**Remark 5.1.1** The condition rank$(L_1 \cap L_2)$ = rank$(L_1)$ or rank$(L_1 \cap L_2)$ = rank $(L_2)$ in lemma 5.1.4 seems to be necessary. As a counterexample, we see the real line $\mathbb{R}$, let $L_1 = \mathbb{Z}$ and $L_2 = \sqrt{2}\mathbb{Z}$, then $L_1 + L_2$ is not a discrete subgroup of $\mathbb{R}$, thus $L_1 + L_2$ is not a lattice in $\mathbb{R}$. Because $L_1 + L_2 = \{n + \sqrt{2}m \big| n \in \mathbb{Z}, m \in \mathbb{Z}\}$ is dense in $\mathbb{R}$ by Dirichlet's theorem (see theorem I of Cassels (1963)).

As a direct consequence, we have the following generalized form of lemma 5.1.4.

**Lemma 5.1.5** *Let $L_1, L_2, \ldots, L_m$ be $m$ lattices of $\mathbb{R}^n$ and*

$$rank(L_1 \cap L_2 \cap \cdots \cap L_m) = rank(L_j) \text{ for some } 1 \leqslant j \leqslant m.$$

*Then $L_1 + L_2 + \cdots + L_m$ is a lattice of $\mathbb{R}^n$.*

***Proof*** Without loss of generality, we assume that

$$\text{rank}(L_1 \cap L_2 \cap \cdots \cap L_m) = \text{rank}(L_m).$$

Let $L_1 + L_2 + \cdots + L_{m-1} = L'$, then

$$L' + L_m / L' \cong L_m / L' \cap L_m.$$

Since $\text{rank}(L' \cap L_m) = \text{rank}(L_m)$, by lemma 5.1.4, we have $L' + L_m = L_1 + L_2 + \cdots + L_m$ is a lattice of $\mathbb{R}^n$ and lemma 5.1.5 follows. □

## 5.2 Ideal Matrices

In Chap. 3 we introduced the concept of circulant matrix and some related properties. In this section, we generalize them to general ideal matrix and introduce the properties of ideal matrix. By using the characteristic polynomial $\phi(x)$ as modulo and the definition of $\phi$-convolutional product, we establish the ring isomorphism one-to-one correspondence between polynomial quotient rings and $n$ dimensional vectors in $\mathbb{R}^n$.

Let $\mathbb{R}[x]$ and $\mathbb{Z}[x]$ be the polynomial rings over $\mathbb{R}$ and $\mathbb{Z}$ with variable $x$, respectively. Suppose that

$$\phi(x) = x^n - \phi_{n-1}x^{n-1} - \cdots - \phi_1 x - \phi_0 \in \mathbb{Z}[x],\ \phi_0 \neq 0 \tag{5.2.1}$$

is a polynomial with integer coefficients of which has no multiple roots in complex number field $\mathbb{C}$. Let $w_1, w_2, \ldots, w_n$ be the $n$ different roots of $\phi(x)$ in $\mathbb{C}$, the Vandermonde matrix $V_\phi$ is defined by

$$V_\phi = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ w_1 & w_2 & \cdots & w_n \\ \vdots & \vdots & & \vdots \\ w_1^{n-1} & w_2^{n-1} & \cdots & w_n^{n-1} \end{pmatrix}, \quad \det(V_\phi) \neq 0. \tag{5.2.2}$$

According to the given polynomial $\phi(x)$, we define a rotation matrix $H = H_\phi$ by

$$H = H_\phi = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & \phi_0 \\ \hline & & & \phi_1 \\ & I_{n-1} & & \vdots \\ & & & \phi_{n-1} \end{array}\right)_{n\times n} \in \mathbb{Z}^{n\times n}, \tag{5.2.3}$$

where $I_{n-1}$ is the $(n-1) \times (n-1)$ unit matrix. Obviously, the characteristic polynomial of $H$ is just $\phi(x)$. We use column notation for vectors in $\mathbb{R}^n$. Let $\{e_0, e_1, \ldots, e_{n-1}\}$ be the standard basis of $\mathbb{R}^n$, see (5.1.2) in Chap. 3.

**Definition 5.2.1** For any $f = \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix} \in \mathbb{R}^n$, the ideal matrix generated by vector $f$ is defined by

$$H^*(f) = [f, Hf, H^2 f, \ldots, H^{n-1} f]_{n \times n} \in \mathbb{R}^{n \times n}, \tag{5.2.4}$$

which is a block matrix in terms of each column $H^k f$ $(0 \leqslant k \leqslant n-1)$. Sometimes, $f$ is called an input vector. In Chap. 3, we introduced the definition of circulant matrix. It is easily seen that $H^*(f)$ is a more general form of the classical circulant matrix and $r$-circulant matrix (Shi, 2018; Yasin and Taskara, 2013). In fact, if $\phi(x) = x^n - 1$, then $H^*(f)$ is the ordinary circulant matrix generated by $f$. If $\phi(x) = x^n - r$, then $H^*(f)$ is the $r$-circulant matrix.

By (5.2.4), it follows immediately that

$$H^*(f + g) = H^*(f) + H^*(g), \tag{5.2.5}$$

and

$$H^*(\lambda f) = \lambda H^*(f), \ \forall \lambda \in \mathbb{R}. \tag{5.2.6}$$

Specially, for any $f = \begin{pmatrix} f_0 \\ \vdots \\ f_{n-1} \end{pmatrix} \in \mathbb{R}^n$, the ideal matrix $H^*(f)$ generated by $f$ could be written as

$$H^*(f) = H^* \left( \sum_{i=0}^{n-1} f_i e_i \right) = \sum_{i=0}^{n-1} f_i H^*(e_i),$$

which means that any ideal matrix is the linear combination of ideal matrices generated by the standard basis vectors $e_i$. It is easy to verify that

$$H^*(e_0) = I_n, \ H^*(e_k) = H^k, \ 1 \leqslant k \leqslant n-1,$$

So the unit matrix $I_n$ and rotation matrices $H^k$ $(1 \leqslant k \leqslant n-1)$ are all the ideal matrices.

Moreover, $H^*(f) = 0$ is a zero matrix if and only if $f = 0$ is a zero vector, thus one has $H^*(f) = H^*(g)$ if and only if $f = g$. Let $M^*$ be the set of all ideal matrices, namely

$$M^* = \{H^*(f) \mid f \in \mathbb{R}^n\}. \tag{5.2.7}$$

We may regard $H^*$ as a mapping from $\mathbb{R}^n$ to $M^*$ of which is a one-to-one correspondence. Next we show some basic properties for ideal matrix, and more contents could be found in Zheng et al. (2022a).

**Lemma 5.2.1** *For any $f \in \mathbb{R}^n$, we have*

$$H \cdot H^*(f) = H^*(f) \cdot H. \tag{5.2.8}$$

***Proof*** Since $\phi(x) = x^n - \phi_{n-1}x^{n-1} - \cdots - \phi_1 x - \phi_0$ is the characteristic polynomial of $H$, by Hamilton–Cayley theorem, we have

$$H^n = \phi_0 I_n + \phi_1 H + \cdots + \phi_{n-1}H^{n-1}.$$

Let

$$b = \begin{pmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_{n-1} \end{pmatrix} \text{ and } H = \begin{pmatrix} 0 & \phi_0 \\ I_{n-1} & b \end{pmatrix}.$$

By (5.2.4) we have

$$\begin{aligned} H^*(f)H &= [f, Hf, ..., H^{n-1}f]\begin{pmatrix} 0 & \phi_0 \\ I_{n-1} & b \end{pmatrix} \\ &= [Hf, H^2 f, ..., H^{n-1}f, \phi_0 f + \phi_1 Hf + \cdots + \phi_{n-1}H^{n-1}f] \\ &= [Hf, H^2 f, ..., H^{n-1}f, H^n f] \\ &= H[f, Hf, ..., H^{n-1}f] = H \cdot H^*(f), \end{aligned}$$

The lemma follows. □

**Lemma 5.2.2** *For any $f = \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix} \in \mathbb{R}^n$ we have*

$$H^*(f) = f_0 I_n + f_1 H + \cdots + f_{n-1}H^{n-1}. \tag{5.2.9}$$

***Proof*** We use induction on $n$ to show this conclusion. If $n = 1$, it is trivial. Suppose it is true for $n$, we consider the case of $n + 1$. For this purpose, we write $H = H_n$, $e_0, e_1, ..., e_{n-1}$ the $n$ column vectors of unit in $\mathbb{R}^n$, namely

$$e_0 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_1 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \cdots e_{n-1} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

and

$$H_{n+1} = \begin{pmatrix} 0 & A_0 \\ e_0 & Hn \end{pmatrix},$$

where $A_0 = (0, 0, ..., \phi_0) \in \mathbb{R}^n$ is a row vector. For any $k$, $1 \leqslant k \leqslant n-1$, it is easy to check that

$$H_n e_{k-1} = e_k,\ H_n^k e_0 = e_k \text{ and } H_{n+1}^k = \begin{pmatrix} 0 & A_0 H_n^{k-1} \\ e_{k-1} & H_n^k \end{pmatrix}.$$

Let $f = \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \\ f_n \end{pmatrix} \in \mathbb{R}^{n+1}$, we denote $f'$ by

$$f' = \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix} \in \mathbb{R}^n,\ f = \begin{pmatrix} f_0 \\ f' \end{pmatrix}.$$

By the assumption of induction, we have

$$H_n^*(f') = [f', H_n f', ..., H_n^{n-1} f'] = f_1 I_n + f_2 H_n + \cdots + f_n H_n^{n-1},$$

it follows that

$$\begin{aligned} H_{n+1}^*(f) &= \left[ \begin{pmatrix} f_0 \\ f' \end{pmatrix}, H_{n+1} \begin{pmatrix} f_0 \\ f' \end{pmatrix}, \ldots, H_{n+1}^n \begin{pmatrix} f_0 \\ f' \end{pmatrix} \right] \\ &= f_0 I_n + f_1 H_{n+1} + \cdots + f_n H_{n+1}^n. \end{aligned}$$

We complete the proof of lemma 5.2.2. □

**Lemma 5.2.3** *Let $f(x) = f_0 + f_1 x + \cdots + f_{n-1} x^{n-1} \in \mathbb{R}[x]$, then we have*

$$H^*(f) = V_\phi^{-1} diag\{f(w_1), f(w_2), ..., f(w_n)\} V_\phi, \tag{5.2.10}$$

*where $diag\{f(w_1), f(w_2), ..., f(w_n)\}$ is the diagonal matrix.*

***Proof*** By theorem 3.2.5 of Davis (1994), for $H$, we have

$$H = V_\phi^{-1} \text{diag}\{w_1, w_2, ..., w_n\} V_\phi,$$

By lemma 5.2.2, it follows that

$$H^*(f) = V_\phi^{-1} \text{ diag } \{f(w_1), f(w_2), ..., f(w_n)\} V_\phi.$$

□

Now, we summarize some basic properties for ideal matrix as follows.

**Lemma 5.2.4** *Suppose $\phi(x) \in \mathbb{Z}[x]$ is a polynomial of which has no multiple roots in complex number field $\mathbb{C}$. $f \in \mathbb{R}^n$, $g \in \mathbb{R}^n$ be two column vectors, we have*

*(i)* $H^*(f)H^*(g) = H^*(g)H^*(f)$;
*(ii)* $H^*(f)H^*(g) = H^*(H^*(f)g)$;
*(iii)* $det(H^*(f)) = \Pi_{i=1}^n f(w_i)$;
*(iv)* $H^*(f)$ *is an invertible matrix if and only if* $\phi(x)$ *and* $f(x)$ *are coprime, i.e. gcd* $(\phi(x), f(x)) = 1$.

***Proof*** (i) and (ii) follow from lemma 5.2.2 immediately, (iii) and (iv) follow from lemma 5.2.3. □

In Sect. 3.1, we took the characteristic polynomial $x^n - 1$ as modulo and constructed the one-to-one correspondence between polynomial quotient rings and $n$ dimensional vectors. Now we can generalize it to the general case using characteristic polynomial $\phi(x)$ as modulo. Let $\phi(x)\mathbb{R}[x]$ and $\phi(x)\mathbb{Z}[x]$ be the principal ideals generated by $\phi(x)$ in $\mathbb{R}[x]$ and $\mathbb{Z}[x]$, respectively, we denote the quotient rings $R$ and $\overline{R}$ by

$$R = \mathbb{Z}[x]/\phi(x)\mathbb{Z}[x], \ \overline{R} = \mathbb{R}[x]/\phi(x)\mathbb{R}[x]. \tag{5.2.11}$$

There is a one-to-one correspondence between $\overline{R}$ and $\mathbb{R}^n$ given by

$$f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} \in \overline{R} \longleftrightarrow f = \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix} \in \mathbb{R}^n. \tag{5.2.12}$$

We denote this correspondence by $t$, that is

$$t(f(x)) = f, \ t^{-1}(f) = f(x). \tag{5.2.13}$$

If we restrict $t$ in the quotient ring $R$, then which gives a one-to-one correspondence between $R$ and $\mathbb{Z}^n$. First, we show that $t$ is also a ring isomorphism.

**Definition 5.2.2** For any two column vectors $f$ and $g$ in $\mathbb{R}^n$, we define the $\phi$-convolutional product $f * g$ by

$$f * g = H^*(f)g. \tag{5.2.14}$$

By lemma 5.2.4, it is easy to see that

$$f * g = g * f, \text{ and } H^*(f * g) = H^*(f)H^*(g).$$

**Lemma 5.2.5** *For any two polynomials $f(x)$ and $g(x)$ in $\overline{R}$, we have*

$$t(f(x)g(x)) = H^*(f)g = f * g. \tag{5.2.15}$$

***Proof*** Let $g(x) = g_0 + g_1 x + \cdots + g_{n-1}x^{n-1} \in \overline{R}$, then

$$xg(x) = \phi_0 g_{n-1} + (g_0 + \phi_1 g_{n-1})x + \cdots + (g_{n-2} + \phi_{n-1}g_{n-1})x^{n-1},$$

it follows that

$$t(xg(x)) = Ht(g(x)) = Hg. \tag{5.2.16}$$

Hence, for any $0 \leqslant k \leqslant n-1$, we have

$$t(x^k g(x)) = H^k t(g(x)) = H^k g,\ 0 \leqslant k \leqslant n-1.$$

Let $f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} \in \overline{R}$, by lemma 5.2.2, we have

$$t(f(x)g(x)) = \sum_{i=0}^{n-1} f_i t(x^i g(x)) = \sum_{i=0}^{n-1} f_i H^i g = H^*(f)g.$$

The lemma follows. □

**Lemma 5.2.6** *Under $\phi$-convolutional product, $\mathbb{R}^n$ is a commutative ring with identity element $e_0$ and $\mathbb{Z}^n \subset \mathbb{R}^n$ is its subring. Moreover, we have the following ring isomorphisms*

$$\overline{R} \cong \mathbb{R}^n \cong M^*,\ R \cong \mathbb{Z}^n \cong M_{\mathbb{Z}}^*,$$

*where $M^*$ is the set of all ideal matrices given by (5.2.7), and $M_{\mathbb{Z}}^*$ is the set of all integer ideal matrices.*

***Proof*** Let $f(x) \in \overline{R}$ and $g(x) \in \overline{R}$, then

$$t(f(x) + g(x)) = f + g = t(f(x)) + t(g(x)),$$

and

$$t(f(x)g(x)) = H^*(f)g = f * g = t(f(x)) * t(g(x)),$$

this means that $t$ is a ring isomorphism. Since $f * g = g * f$ and $e_0 * g = H^*(e_0)g = I_n g = g$, then $\mathbb{R}^n$ is a commutative ring with $e_0$ as the identity elements. Noting $H^*(f)$ is an integer matrix if and only if $f \in \mathbb{Z}^n$ is an integer vector, the isomorphism of subrings follows immediately. □

According to property (iv) of lemma 5.2.4, $H^*(f)$ is an invertible matrix whenever $(f(x), \phi(x)) = 1$ in $\mathbb{R}[x]$, we show that the inverse of an ideal matrix is again an ideal matrix.

**Lemma 5.2.7** *Let $f(x) \in \overline{R}$ and $(f(x), \phi(x)) = 1$ in $\mathbb{R}[x]$, then*

$$(H^*(f))^{-1} = H^*(u),$$

*where $u(x) \in \overline{R}$ is the unique polynomial such that $u(x)f(x) \equiv 1 \ (mod\ \phi(x))$.*

***Proof*** By lemma 5.2.5, we have $u * f = e_0$, it follows that

$$H^*(u)H^*(f) = H^*(e_0) = I_n,$$

thus we have $(H^*(f))^{-1} = H^*(u)$. It is worth to note that if $H^*(f)$ is an invertible integer matrix, then $(H^*(f))^{-1}$ is not an integer matrix in general. □

Sometimes, the following lemma may be useful, especially, when we consider an integer matrix.

**Lemma 5.2.8** *Let $f(x) \in \mathbb{Z}[x]$ and $(f(x), \phi(x)) = 1$ in $\mathbb{Z}[x]$, then we have $(f(x), \phi(x)) = 1$ in $\mathbb{R}[x]$.*

***Proof*** Let $\mathbb{Q}$ be the rational number field. Since $(f(x), \phi(x)) = 1$ in $\mathbb{Z}[x]$, then $(f(x), \phi(x)) = 1$ in $\mathbb{Q}[x]$. We know that $\mathbb{Q}[x]$ is a principal ideal domain, thus there are two polynomials $a(x)$ and $b(x)$ in $\mathbb{Q}[x]$ such that

$$a(x)f(x) + b(x)\phi(x) = 1.$$

This means that $(f(x), \phi(x)) = 1$ in $\mathbb{R}[x]$. □

## 5.3 $\phi$-Cyclic Lattice

As we know that cyclic code plays a central role in algebraic coding theorem (see Chap. 6 of Lint (1999)). In Zheng et al. (2022a), we extended ordinary cyclic code to more general forms, namely $\phi$-cyclic codes, which will be introduced in Chap. 7. To obtain an analogous concept of $\phi$-cyclic code in $\mathbb{R}^n$, we note that every rotation matrix $H$ defines a linear transformation of $\mathbb{R}^n$ by $x \to Hx$.

**Definition 5.3.1** $H$ is the rotation matrix defined in (5.2.3). A linear subspace $C \subset \mathbb{R}^n$ is called a $\phi$-cyclic subspace if $\forall \alpha \in C \Rightarrow H\alpha \in C$. A lattice $L \subset \mathbb{R}^n$ is called a $\phi$-cyclic lattice if $\forall \alpha \in L \Rightarrow H\alpha \in L$.

In other words, a $\phi$-cyclic subspace $C$ is a linear subspace of $\mathbb{R}^n$, of which is closed under linear transformation $H$. A $\phi$-cyclic lattice $L$ is a lattice of $\mathbb{R}^n$ of which

is closed under $H$. If $\phi(x) = x^n - 1$, then $H$ is the classical circulant matrix and the corresponding cyclic lattice was first appeared in Micciancio Micciancio (2002), but he does not discuss the further property for these lattices. To obtain the explicit algebraic construction of $\phi$-cyclic lattice, we first show that there is a one-to-one correspondence between $\phi$-cyclic subspaces of $\mathbb{R}^n$ and the ideals of $\overline{R}$.

**Lemma 5.3.1** *Let $t$ be the correspondence between $\overline{R}$ and $\mathbb{R}^n$ given by (5.2.13), then a subset $C \subset \mathbb{R}^n$ is a $\phi$-cyclic subspace of $\mathbb{R}^n$, if and only if $t^{-1}(C) \subset \overline{R}$ is an ideal.*

***Proof*** We extend the correspondence $t$ to subsets of $\overline{R}$ and $\mathbb{R}^n$ by

$$C(x) \subset \overline{R} \xrightarrow{t} C = \{c \mid c(x) \in C(x)\} \subset \mathbb{R}^n. \tag{5.3.1}$$

Let $C(x) \subset \overline{R}$ be an ideal, it is clear that $C \subset t(C(x))$ is a linear subspace of $\mathbb{R}^n$. To prove $C$ is a $\phi$-cyclic subspace, we note that if $c(x) \in C(x)$, then by (5.2.16)

$$xc(x) \in C(x) \Leftrightarrow Ht(c(x)) = Hc \in C.$$

Therefore, if $C(x)$ is an ideal of $\overline{R}$, then $t(C(x)) = C$ is a $\phi$-cyclic subspace of $\mathbb{R}^n$. Conversely, if $C \subset \mathbb{R}^n$ is a $\phi$-cyclic subspace, then for any $k \geqslant 1$, we have $H^k c \in C$ whenever $c \in C$, it implies

$$\forall c(x) \in C(x) \Rightarrow x^k c(x) \in C(x),\ 0 \leqslant k \leqslant n-1,$$

which means that $C(x)$ is an ideal of $\overline{R}$. We complete the proof. □

By the above lemma, to find a $\phi$-cyclic subspace in $\mathbb{R}^n$, it is enough to find an ideal of $\overline{R}$. There are two trivial ideals $C(x) = 0$ and $C(x) = \overline{R}$, the corresponding $\phi$-cyclic subspace are $C = 0$ and $C = \mathbb{R}^n$. To find non-trivial $\phi$-cyclic subspaces, we make use of the homomorphism theorems, which is a standard technique in algebra. Let $\pi$ be the natural homomorphism from $\mathbb{R}[x]$ to $\overline{R}$, $\ker\pi = \phi(x)\mathbb{R}[x]$. We write $\phi(x)\mathbb{R}[x]$ by $< \phi(x) >$. Let $N$ be an ideal of $\mathbb{R}[x]$ satisfying

$$< \phi(x) > \subset N \subset \mathbb{R}[x] \xrightarrow{\pi} \overline{R} = \mathbb{R}[x]/ < \phi(x) > . \tag{5.3.2}$$

Since $\mathbb{R}[x]$ is a principal ideal domain, then $N =< g(x) >$ is a principal ideal generated by a monic polynomial $g(x) \in \mathbb{R}[x]$. It is easy to see that

$$< \phi(x) > \subset < g(x) > \Leftrightarrow g(x) | \phi(x) \text{ in } \mathbb{R}[x].$$

It follows that all ideals $N$ satisfying (5.3.2) are given by

$$\{< g(x) > \mid g(x) \in \mathbb{R}[x] \text{ is monic and } g(x) | \phi(x)\}.$$

We write by $< g(x) > \bmod \phi(x)$, the image of $< g(x) >$ under $\pi$, i.e.

$$< g(x) > \bmod \phi(x) = \pi(< g(x) >).$$

It is easy to check

$$< g(x) > \bmod \phi(x) = \{a(x)g(x) \mid a(x) \in \mathbb{R}[x] \text{ and } \deg a(x) + \deg g(x) < n\}. \tag{5.3.3}$$

more precisely, which is a representative elements set of $< g(x) > \bmod \phi(x)$. By homomorphism theorem in ring theory, all ideals of $\overline{R}$ given by

$$\{< g(x) > \bmod \phi(x) \mid g(x) \in \mathbb{R}[x] \text{ is monic and } g(x)|\phi(x)\}. \tag{5.3.4}$$

Let $d$ be the number of monic divisors of $\phi(x)$ in $\mathbb{R}[x]$, we have the following lemma.

**Lemma 5.3.2** *The number of $\phi$-cyclic subspace of $\mathbb{R}^n$ is $d$.*

***Proof*** By lemma 5.3.1, the correspondence between $\phi$-cyclic subspace of $\mathbb{R}^n$ and ideal of $\overline{R}$ is one-to-one. Based on (5.3.4), the number of ideal of $\overline{R}$ is equal to the number of divisors of $\phi(x)$ in $\mathbb{R}[x]$, i.e. $d$. So the number of $\phi$-cyclic subspace of $\mathbb{R}^n$ is $d$. □

Next, we discuss $\phi$-cyclic lattice, which is the geometric analogy of cyclic code. The $\phi$-cyclic subspace of $\mathbb{R}^n$ maybe regarded as the algebraic analogy of cyclic code. Let the quotient rings $R$ and $\overline{R}$ given by (5.2.11). A $R$-module is an Abel group $\Lambda$ such that there is an operator $\lambda\alpha \in \Lambda$ for all $\lambda \in R$ and $\alpha \in \Lambda$, satisfying $1 \cdot \alpha = \alpha$ and $(\lambda_1\lambda_2)\alpha = \lambda_1(\lambda_2\alpha)$. It is easy to see that $\overline{R}$ is a $R$-module, if $\Lambda \subset \overline{R}$ and $\Lambda$ is a $R$-module, then $\Lambda$ is called a $R$-submodule of $\overline{R}$. All $R$-modules we discuss here are $R$-submodule of $\overline{R}$. On the other hand, if $I \subset R$, then $I$ is an ideal of $R$, if and only if $I$ is a $R$-module. Let $\alpha \in \overline{R}$, the cyclic $R$-module generated by $\alpha$ be defined by

$$R\alpha = \{\lambda\alpha \mid \lambda \in R\}. \tag{5.3.5}$$

If there are finitely many polynomials $\alpha_1, \alpha_2, \ldots, \alpha_k$ in $\overline{R}$ such that

$$\Lambda = R\alpha_1 + R\alpha_2 + \cdots + R\alpha_k,$$

then $\Lambda$ is called a finitely generated $R$-module, which is a $R$-submodule of $\overline{R}$.

Now, if $L \subset \mathbb{R}^n$ is a $\phi$-cyclic lattice, $g \in \mathbb{R}^n$, $H^*(g)$ is the ideal matrix generated by vector $g$, and $L(H^*(g))$ is the lattice generated by $H^*(g)$. In the following lemma, we prove that any $L(H^*(g))$ is a $\phi$-cyclic lattice and

$$g \in L \Rightarrow L(H^*(g)) \subset L, \tag{5.3.6}$$

which implies that $L(H^*(g))$ is the smallest $\phi$-cyclic lattice of which contains vector $g$. Therefore, we call $L(H^*(g))$ is a minimal $\phi$-cyclic lattice in $\mathbb{R}^n$.

**Lemma 5.3.3** *For any vector $g \in \mathbb{R}^n$, then $L(H^*(g))$ is a $\phi$-cyclic lattice. Moreover, if $L \subset \mathbb{R}^n$ is a $\phi$-cyclic lattice and $g \in L$, then we have $L(H^*(g)) \subset L$.*

***Proof*** Let $\alpha \in H^*(g)$, then there is an integer vector $b \in \mathbb{Z}^n$ such that $\alpha = H^*(g)b$. By lemma 5.2.2, we have

$$\alpha = g_0 I_n b + g_1 H b + \cdots + g_{n-1} H^{n-1} b$$

and

$$H\alpha = (g_0 I_n + g_1 H + \cdots + g_{n-1} H^{n-1}) H b = H^*(g) H b.$$

Since $Hb \in \mathbb{Z}^n$, it follows that $H\alpha \in L(H^*(g))$. This means that $L(H^*(g))$ is a $\phi$-cyclic lattice. If $L$ is a $\phi$-cyclic lattice and $g \in L$, then $H^k g \in L$ for $0 \leqslant k \leqslant n-1$, and

$$b_0 I_n g + b_1 H g + \cdots + b_{n-1} H^{n-1} g \in L, \text{ for all } b = \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} \in \mathbb{Z}^n.$$

It follows that

$$H^*(b)g = H^*(g)b \in L, \quad b \in \mathbb{Z}^n.$$

Thus we have $L(H^*(g)) \subset L$, and lemma 5.3.3 holds. □

**Lemma 5.3.4** *There is a one-to-one correspondence between the minimal $\phi$-cyclic lattice in $\mathbb{R}^n$ and the cyclic $R$-submodule in $\overline{R}$, namely*

$$t(Rg(x)) = L(H^*(g)), \text{ for all } g(x) \in \overline{R}$$

*and*

$$t^{-1}(L(H^*(g))) = Rg(x), \text{ for all } g \in \mathbb{R}^n.$$

***Proof*** Let $b(x) \in R$, by lemma 5.2.5, we have

$$t(b(x)g(x)) = H^*(b)g = H^*(g)b \in L(H^*(g)),$$

and $t(Rg(x)) \subset L(H^*(g))$. Conversely, if $\alpha \in L(H^*(g))$, and $\alpha = H^*(g)b$ for some integer vector $b$, by lemma 5.2.5 again, we have $b(x)g(x) \in Rg(x)$, and $t(b(x)g(x)) = \alpha$. This implies that

$$L(H^*(g)) \subset t(Rg(x)),$$

and

$$t(Rg(x)) = L(H^*(g)).$$

The lemma follows immediately. □

Suppose $L = L(\beta_1, \beta_2, \ldots, \beta_m)$ is arbitrary $\phi$-cyclic lattice, where $B = [\beta_1, \beta_2, \ldots, \beta_m]_{n\times m}$ is the generated matrix of $L$. $L$ may be expressed as the sum of finitely many minimal $\phi$-cyclic lattices, in fact, we have

$$L = L(H^*(\beta_1)) + L(H^*(\beta_2)) + \cdots + L(H^*(\beta_m)). \tag{5.3.7}$$

To state and prove our main results, first, we give a definition of prime spot in $\mathbb{R}^n$.

**Definition 5.3.2** Let $g \in \mathbb{R}^n$, and $g(x) = t^{-1}(g) \in \overline{R}$. If $(g(x), \phi(x)) = 1$ in $\mathbb{R}[x]$, we call $g$ is a prime spot of $\mathbb{R}^n$.

By (iv) of lemma 5.2.4, $g \in \mathbb{R}^n$ is a prime spot if and only if $H^*(g)$ is an invertible matrix, thus the minimal $\phi$-cyclic lattice $L(H^*(g))$ generated by a prime spot is a full-rank lattice.

**Lemma 5.3.5** *Let $g$ and $f$ be two prime spots of $\mathbb{R}^n$, then $L(H^*(g)) + L(H^*(f))$ is a full-rank $\phi$-cyclic lattice.*

***Proof*** According to lemma 5.1.4, it is sufficient to show that

$$\operatorname{rank}\big(L(H^*(g)) \cap L(H^*(f))\big) = \operatorname{rank}\big(L(H^*(g))\big) = n. \tag{5.3.8}$$

In fact, we should prove in general

$$L(H^*(g) \cdot H^*(f)) \subset L(H^*(g)) \cap L(H^*(f)). \tag{5.3.9}$$

If (5.3.9) holds, since $H^*(g) \cdot H^*(f)$ is invertible matrix, then

$$\operatorname{rank}\big(L(H^*(g) \cdot H^*(f))\big) = n,$$

(5.3.8) holds. To prove (5.3.9), we note that

$$L(H^*(g) \cdot H^*(f)) = L(H^*(g * f)),$$

It follows that

$$t^{-1}\big(L(H^*(g) \cdot H^*(f))\big) = Rg(x)f(x),$$

It is easy to see that

$$Rg(x)f(x) \subset Rg(x) \cap Rf(x).$$

Therefore, we have

$$L(H^*(g) \cdot H^*(f)) = t(Rg(x)f(x)) \subset L(H^*(g)) \cap L(H^*(f)).$$

This is the proof of lemma 5.3.5. □

It is worth to note that (5.3.9) is true for more general case and does not need the condition of prime spot. We have the following lemma.

**Lemma 5.3.6** *Let $\beta_1, \beta_2, \ldots, \beta_m$ be arbitrary $m$ vectors in $\mathbb{R}^n$, then we have*

$$L(H^*(\beta_1)H^*(\beta_2)\cdots H^*(\beta_m)) \subset L(H^*(\beta_1)) \cap L(H^*(\beta_2)) \cap \cdots \cap L(H^*(\beta_m)). \tag{5.3.10}$$

***Proof*** If $\beta_1, \beta_2, \ldots, \beta_m$ are integer vectors, then (5.3.10) is trivial. For the general case, we write

$$L(H^*(\beta_1) \cdot H^*(\beta_2)\cdots H^*(\beta_m)) = L(H^*(\beta_1 * \beta_2 * \cdots * \beta_m)),$$

where $\beta_1 * \beta_2 * \cdots * \beta_m$ is the $\phi$-convolutional product defined in (5.2.14), then

$$t^{-1}\big(L(H^*(\beta_1)\cdots H^*(\beta_m))\big) = R\beta_1(x)\beta_2(x)\cdots\beta_m(x).$$

Since

$$R\beta_1(x)\beta_2(x)\cdots\beta_m(x) \subset R\beta_1(x) \cap R\beta_2(x) \cap \cdots \cap R\beta_m(x),$$

It follows that

$$L(H^*(\beta_1)H^*(\beta_2)\cdots H^*(\beta_m)) \subset L(H^*(\beta_1)) \cap L(H^*(\beta_2)) \cap \cdots \cap L(H^*(\beta_m)).$$

We have this lemma. □

By lemma 5.3.5, we also have the following corollary.

**Corollary 5.3.1** *Let $\beta_1, \beta_2, \ldots, \beta_m$ be $m$ prime spots of $\mathbb{R}^n$, then $L(H^*(\beta_1)) + L(H^*(\beta_2)) + \cdots + L(H^*(\beta_m))$ is a full-rank $\phi$-cyclic lattice.*

***Proof*** Based on lemma 5.1.5, it follows immediately from lemma 5.3.5. □

Our main result in this paper is to establish the following one-to-one correspondence between $\phi$-cyclic lattices in $\mathbb{R}^n$ and finitely generated $R$-modules in $\overline{R}$.

**Theorem 5.3.1** *Let $\Lambda = R\alpha_1(x) + R\alpha_2(x) + \cdots + R\alpha_m(x)$ be a finitely generated $R$-module in $\overline{R}$, then $t(\Lambda)$ is a $\phi$-cyclic lattice in $\mathbb{R}^n$. Conversely, if $L \subset \mathbb{R}^n$ is a $\phi$-cyclic lattice in $\mathbb{R}^n$, then $t^{-1}(L)$ is a finitely generated $R$-module in $\overline{R}$, that is a one-to-one correspondence.*

***Proof*** If $\Lambda$ is a finitely generated $R$-module, by lemma 5.3.4, we have

$$\begin{aligned} t(\Lambda) &= t(R\alpha_1(x) + \cdots + R\alpha_m(x)) \\ &= L(H^*(\alpha_1)) + L(H^*(\alpha_2)) + \cdots + L(H^*(\alpha_m)). \end{aligned}$$

The main difficult is to show that $t(\Lambda)$ is a lattice of $\mathbb{R}^n$, we require a surgery to embed $t(\Lambda)$ into a full-rank lattice. To do this, let $(\alpha_i(x), \phi(x)) = d_i(x)$, $d_i(x) \in \mathbb{Z}[x]$, and

$\beta_i(x) = \alpha_i(x)/d_i(x)$, $1 \leqslant i \leqslant m$. Since $\phi(x)$ has no multiple roots by assumption, then $(\beta_i(x), \phi(x)) = 1$ in $\mathbb{R}[x]$. In other words, each $t(\beta_i(x)) = \beta_i$ is a prime spot. It is easy to verify $R\alpha_i(x) \subset R\beta_i(x)$ $(1 \leqslant i \leqslant m)$, thus we have

$$t(\Lambda) \subset L(H^*(\beta_1)) + L(H^*(\beta_2)) + \cdots + L(H^*(\beta_m)).$$

By corollary 5.3.1, we have $t(\Lambda)$ is $\phi$-cyclic lattice. Conversely, if $L \subset \mathbb{R}^n$ is a $\phi$-cyclic lattice of $\mathbb{R}^n$, and $L = L(\beta_1, \beta_2, \ldots, \beta_m)$, by (5.3.7), we have

$$t^{-1}(L) = R\beta_1(x) + R\beta_2(x) + \cdots + R\beta_m(x),$$

which is a finitely generated $R$-module in $\overline{R}$. We complete the proof of theorem 5.3.1. □

Since $R$ is a Noether ring, then $I \subset R$ is an ideal if and only if $I$ is a finitely generated $R$-module. On the other hand, if $I \subset R$ is an ideal, then $t(I) \subset \mathbb{Z}^n$ is a discrete subgroup of $\mathbb{Z}^n$, thus $t(I)$ is a lattice. We give the following definition.

**Definition 5.3.3** Let $I \subset R$ be an ideal, $t(I)$ is called the $\phi$-ideal lattice.

Ideal lattice was first appeared in Lyubashevsky and Micciancio (2006), and more contents could be found in Zheng et al. (2022a). As a direct consequence of theorem 5.3.1, we have the following corollary.

**Corollary 5.3.2** *Let $L \subset \mathbb{R}^n$ be a subset, then $L$ is a $\phi$-cyclic lattice if and only if*

$$L = L(H^*(\beta_1)) + L(H^*(\beta_2)) + \cdots + L(H^*(\beta_m)),$$

*where $\beta_i \in \mathbb{R}^n$ and $m \leqslant n$. Furthermore, $L$ is a $\phi$-ideal lattice if and only if every $\beta_i \in \mathbb{Z}^n$, $1 \leqslant i \leqslant m$.*

**Corollary 5.3.3** *Suppose that $\phi(x)$ is an irreducible polynomial in $\mathbb{Z}[x]$, then any nonzero ideal $I$ of $R$ defines a full-rank $\phi$-ideal lattice $t(I) \subset \mathbb{Z}^n$.*

***Proof*** Let $I \subset R$ be a nonzero ideal, then we have $I = R\alpha_1(x) + R\alpha_2(x) + \cdots + R\alpha_m(x)$, where $\alpha_i(x) \in R$ and $(\alpha_i(x), \phi(x)) = 1$. It follows that

$$t(I) = L(H^*(\alpha_1)) + L(H^*(\alpha_2)) + \cdots + L(H^*(\alpha_m)).$$

Since each $\alpha_i$ is a prime spot, we have $\operatorname{rank}(t(I)) = n$ by corollary 5.3.1, and the corollary follows at once. □

We have proved that any an ideal of $R$ corresponding to a $\phi$-ideal lattice, which just is a $\phi$-cyclic integer lattice under the more general rotation matrix $H = H_\phi$. Cyclic lattice and ideal lattice were introduced in Lyubashevsky and Micciancio (2006) and Micciancio (2002), respectively, to improve the space complexity of lattice-based cryptosystems. Ideal lattices allow to represent a lattice using only two polynomials. Using such lattices, class lattice-based cryptosystems can diminish

their space complexity from $O(n^2)$ to $O(n)$. Ideal lattices also allow to accelerate computations using the polynomial structure. The original structure of Micciancio's matrices uses the ordinary circulant matrices and allows for an interpretation in terms of arithmetic in polynomial ring $\mathbb{Z}[x]/ < x^n - 1 >$. Lyubashevsky and Micciancio latter suggested to change the ring to $\mathbb{Z}[x]/ < \phi(x) >$ with an irreducible $\phi(x)$ over $\mathbb{Z}[x]$. Our results here suggest to change the ring to $\mathbb{Z}[x]/ < \phi(x) >$ with any a polynomial $\phi(x)$. There are many works subsequent to Lyubashevsky and Micciancio, such as Micciancio and Regev (2009); Peikert (2016).

***Example 5.1*** It is interesting to find some examples of $\phi$-cyclic lattices in an algebraic number field $\mathbb{K}$. Let $\mathbb{Q}$ be rational number field, without loss of generality, an algebraic number field $\mathbb{K}$ of degree $n$ is just $\mathbb{K} = \mathbb{Q}(w)$, where $w = w_i$ is a root of $\phi(x)$. If all $\mathbb{Q}(w_i) \subset \mathbb{R}$ $(1 \leqslant i \leqslant n)$, then $\mathbb{K}$ is called a totally real algebraic number field. Let $O_{\mathbb{K}}$ be the ring of algebraic integers of $\mathbb{K}$, and $I \subset O_{\mathbb{K}}$ be an ideal, $I \neq 0$. Since there is an integral basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subset I$ such that

$$I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n,$$

We may regard every ideal of $O_{\mathbb{K}}$ as a lattice in $\mathbb{Q}^n$, our assertion is that every nonzero ideal of $O_{\mathbb{K}}$ is corresponding to a full-rank $\phi$-cyclic lattice of $\mathbb{Q}^n$. To see this example, let

$$\mathbb{Q}[w] = \left\{ \sum_{i=0}^{n-1} a_i w^i \mid a_i \in \mathbb{Q} \right\},$$

It is known that $\mathbb{K} = \mathbb{Q}[w]$, thus every $\alpha \in \mathbb{K}$ corresponds to a vector $\overline{\alpha} \in \mathbb{Q}^n$ by

$$\alpha = \sum_{i=0}^{n-1} a_i w^i \xrightarrow{\tau} \overline{\alpha} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \in \mathbb{Q}^n.$$

If $I \subset O_{\mathbb{K}}$ is an ideal of $O_{\mathbb{K}}$ and $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$, let $B = [\overline{\alpha_1}, \overline{\alpha_2}, \ldots, \overline{\alpha_n}] \in \mathbb{Q}^{n \times n}$, which is full-rank matrix. We have $\tau(I) = L(B)$ is a full-rank lattice. It remains to show that $\tau(I)$ is a $\phi$-cyclic lattice, we only prove that if $\alpha \in I \Rightarrow H\overline{\alpha} \in \tau(I)$. Suppose that $\alpha \in I$, then $w\alpha \in I$. It is easy to verify that $\tau(w) = e_1$ and

$$\tau(w\alpha) = \tau(w) * \tau(\alpha) = H\overline{\alpha} \in \tau(I).$$

This means that $\tau(I)$ is a $\phi$-cyclic lattice of $\mathbb{Q}^n$, which is a full-rank lattice.

## 5.4 Improved Upper Bound for Smoothing Parameter

As application of the algebraic structure of $\phi$-cyclic lattice, we show that an explicit upper bound of the smoothing parameter for the $\phi$-cyclic lattices. The definition of smoothing parameter was introduced in Chap. 1. Suppose that $L$ is a full-rank lattice and $L^*$ is its dual lattice, for any $\epsilon > 0$, we define the smoothing parameter $\eta_\epsilon(L)$ of $L$ to be the smallest $s$ such that $\rho_{1/s}(L^*) \leqslant 1+\epsilon$, here $\rho$ is the Gauss function,

$$\rho_{s,c}(x) = e^{-\frac{\pi}{s^2}|x-c|^2},\ \rho_s(x) = \rho_{s,0}(x),\ x \in \mathbb{R}^n.$$

Notice that $\rho_{1/s}(L^*)$ is a continuous and strictly decreasing function of $s$, thus the smoothing parameter $\eta_\epsilon(L)$ is a continuous and strictly decreasing function of $\epsilon$, i.e.

$$\eta_{\epsilon_1}(L) \leqslant \eta_{\epsilon_2}(L), \quad \text{if } 0 < \epsilon_2 < \epsilon_1.$$

The following lemma shows the relation of smoothing parameters between a lattice and its sublattice.

**Lemma 5.4.1** *Suppose that $L_1$ and $L_2$ are two full-rank lattices in $\mathbb{R}^n$, and $L_1 \subset L_2$, then for any $\epsilon > 0$, we have*

$$\eta_\epsilon(L_2) \leqslant \eta_\epsilon(L_1). \tag{5.4.1}$$

***Proof*** Let $\eta_\epsilon(L_1) = s$, we are to show that $\eta_\epsilon(L_2) \leqslant s$. Since

$$\rho_{1/s}(L_1^*) = 1+\epsilon,$$

i.e.

$$\sum_{x \in L_1^*} e^{-\pi s^2|x|^2} = 1+\epsilon.$$

It is easy to check that $L_2^* \subset L_1^*$, it follows that

$$1+\epsilon = \sum_{x \in L_1^*} e^{-\pi s^2|x|^2} \geqslant \sum_{x \in L_2^*} e^{-\pi s^2|x|^2},$$

which implies

$$\rho_{1/s}(L_2^*) \leqslant 1+\epsilon,$$

and $\eta_\epsilon(L_2) \leqslant s = \eta_\epsilon(L_1)$, thus we have lemma 5.4.1. □

According to (5.2.4), the ideal matrix $H^*(f)$ with input vector $f \in \mathbb{R}^n$ is just the ordinary circulant matrix when $\phi(x) = x^n - 1$. Next lemma shows that the transpose

of a circulant matrix is still a circulant matrix. For any $g = \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{n-1} \end{pmatrix} \in \mathbb{R}^n$, we denote $\overline{g} = \begin{pmatrix} g_{n-1} \\ g_{n-2} \\ \vdots \\ g_0 \end{pmatrix}$, which is called the conjugation of $g$.

**Lemma 5.4.2** *Let $\phi(x) = x^n - 1$, then for any $g = \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{n-1} \end{pmatrix} \in \mathbb{R}^n$, we have*

$$(H^*(g))^T = H^*(H\overline{g}). \tag{5.4.2}$$

***Proof*** Since $\phi(x) = x^n - 1$, then $H = H_\phi$ is an orthogonal matrix, and we have $H^{-1} = H^{n-1} = H^T$. We write $H_1 = H^T = H^{-1}$. The following identity is easy to verify

$$H^*(g) = \begin{pmatrix} \overline{g}^T H_1 \\ \overline{g}^T H_1^2 \\ \vdots \\ \overline{g}^T H_1^n \end{pmatrix}.$$

It follows that

$$(H^*(g))^T = [H\overline{g}, H(H\overline{g}), \ldots, H^{n-1}(H\overline{g})] = H^*(H\overline{g}),$$

and we have the lemma. □

**Lemma 5.4.3** *Let $\phi(x) = x^n - 1$, suppose that $g \in \mathbb{R}^n$ and the circulant matrix $H^*(g)$ is invertible. Let $A = (H^*(g))^T H^*(g)$, then all characteristic values of $A$ are given by*

$$\{|g(\theta_1)|^2, |g(\theta_2)|^2, \ldots, |g(\theta_n)|^2\},$$

*where $\theta_i^n = 1$ $(1 \leqslant i \leqslant n)$ are the $n$-th roots of unity.*

***Proof*** By lemma 5.4.2 and (ii) of lemma 5.2.4, we have

$$A = H^*(H\overline{g})H^*g = H^*(H^*(H\overline{g})g) = H^*(g''),$$

where $g'' = H^*(H\overline{g})g$. Let $g''(x) = t^{-1}(g'')$ is the corresponding polynomial of $g''$. By lemma 5.2.3, all characteristic values of $A$ are given by

$$\{g''(\theta_1), g''(\theta_2), \ldots, g''(\theta_n)\},\ \theta_i^n = 1,\ 1 \leqslant i \leqslant n.$$

Let $g = \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{n-1} \end{pmatrix} \in \mathbb{R}^n$. It is easy to see that

$$g''(x) = \sum_{i=0}^{n-1} g_i^2 + \left(\sum_{i=0}^{n-1} g_i g_{1-i}\right) x + \cdots + \left(\sum_{i=0}^{n-1} g_i g_{(n-1)-i}\right) x^{n-1} = |g(x)|^2,$$

where $g_{-i} = g_{n-i}$ for all $1 \leqslant i \leqslant n-1$, then the lemma follows at once. □

By the definition of prime spot, if $g \in \mathbb{R}^n$ is a prime spot, then there is a unique polynomial $u(x) \in \overline{R}$ such that $u(x)g(x) \equiv 1 \pmod{\phi(x)}$. We define a new vector $T_g$ and its corresponding polynomial $T_g(x)$ by

$$T_g = H\overline{u},\ T_g(x) = t^{-1}(H\overline{u}). \tag{5.4.3}$$

If $g \in \mathbb{Z}^n$ is an integer vector, then $T_g \in \mathbb{Z}^n$ is also an integer vector, and $T_g(x) \in \mathbb{Z}[x]$ is a polynomial with integer coefficients. Our main result on smoothing parameter is the following theorem.

**Theorem 5.4.1** *Let $\phi(x) = x^n - 1$, $L \subset \mathbb{R}^n$ be a full-rank $\phi$-cyclic lattice, then for any prime spots $g \in L$, we have*

$$\eta_{2^{-n}}(L) \leqslant \sqrt{n}(\min\{|T_g(\theta_1)|, |T_g(\theta_2)|, \ldots, |T_g(\theta_n)|\})^{-1}, \tag{5.4.4}$$

*where $\theta_i^n = 1$, $1 \leqslant i \leqslant n$, and $T_g(x)$ is given by (5.4.3).*

***Proof*** Let $g \in L$ be a prime spot, by lemma 5.4.1, we have

$$L(H^*(g)) \subset L \Rightarrow \eta_\epsilon(L) \leqslant \eta_\epsilon(L(H^*(g))),\ \forall \epsilon > 0.$$

To estimate the smoothing parameter of $L(H^*(g))$, the dual lattice of $L(H^*(g))$ is given by

$$L(H^*(g))^* = L((H^*(u))^T) = L(H^*(H\overline{u})) = L(H^*(T_g)),$$

where $u(x) \in \overline{R}$ and $u(x)g(x) \equiv 1 \pmod{x^n - 1}$, and $T_g$ is given by (5.4.3). Let $A = (H^*(T_g))^T H^*(T_g)$, by lemma 5.4.3, all characteristic values of $A$ are

$$\{|T_g(\theta_1)|^2, |T_g(\theta_2)|^2, \ldots, |T_g(\theta_n)|^2\}.$$

By lemma 5.1.2, the minimum distance $\lambda_1(L(H^*(g))^*)$ is bounded by

$$\lambda_1(L(H^*(g))^*) \geqslant \min\{|T_g(\theta_1)|, |T_g(\theta_2)|, \ldots, |T_g(\theta_n)|\}. \tag{5.4.5}$$

According to the classical estimation of upper bound of smoothing parameter

$$\eta_{2^{-n}}(L) \leqslant \sqrt{n}/\lambda_1(L^*),$$

we see that theorem 5.4.1 holds. □

Let $L = L(B)$ be a full-rank lattice and $B = [\beta_1, \beta_2, \ldots, \beta_n]$. We denote by $B^* = [\beta_1^*, \beta_2^*, \ldots, \beta_n^*]$ the Gram-Schmidt orthogonal vectors $\{\beta_i^*\}$ of the ordered basis $B = \{\beta_i\}$. It is a well-known conclusion that

$$\lambda_1(L) \geqslant |B^*| = \min_{1 \leqslant i \leqslant n} |\beta_i^*|,$$

and

$$\eta_{2^{-n}}(L) \leqslant \sqrt{n}/\lambda_1(L^*),$$

so we get the following upper bound

$$\eta_{2^{-n}}(L) \leqslant \sqrt{n}|B_0^*|^{-1}, \tag{5.4.6}$$

where $B_0^*$ is the orthogonal basis of dual lattice $L^*$ of $L$.

For a $\phi$-cyclic lattice $L$, we observe that the upper bound (5.4.5) is always better than (5.4.6) by numerical testing, we give two examples here.

***Example 5.2*** Let $n = 3$ and $\phi(x) = x^3 - 1$, the rotation matrix $H$ is

$$H = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

We select a $\phi$-cyclic lattice $L = L(B)$, where

$$B = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Since $L = \mathbb{Z}^3$, thus $L$ is a $\phi$-cyclic lattice. It is easy to check

$$|B_0^*| = \min_{1 \leqslant i \leqslant 3} |\beta_i^*| = \frac{\sqrt{3}}{3}.$$

On the other hand, we randomly find a prime spot

$$g = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \in L$$

and $g(x) = x^2$, since

$$xg(x) \equiv 1 \pmod{x^3 - 1},$$

we have

$$T_g(x) = x^2,$$

it follows that

$$|T_g(\theta_1)| = |T_g(\theta_2)| = |T_g(\theta_3)| = 1,$$

and

$$\left( \min_{1 \leqslant i \leqslant 3} |T_g(\theta_i)| \right)^{-1} \leqslant |B_0^*|^{-1} = \sqrt{3}.$$

***Example 5.3*** Let $n = 4$ and $\phi(x) = x^4 - 1$, the rotation matrix $H$ is

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

We select a $\phi$-cyclic lattice $L = L(B)$, where

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Since $L = \mathbb{Z}^4$, thus $L$ is a $\phi$-cyclic lattice. It is easy to check

$$|B_0^*| = \min_{1 \leqslant i \leqslant 4} |\beta_i^*| = \frac{1}{2}.$$

On the other hand, we randomly find a prime spot

$$g = \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix} \in L$$

and $g(x) = x - 2$, since

$$\left(\frac{1}{7}x^3 - \frac{1}{7}x^2 - \frac{2}{7}x - \frac{5}{7}\right) g(x) \equiv 1 \pmod{x^4 - 1},$$

we have

$$T_g(x) = -\frac{2}{7}x^3 - \frac{1}{7}x^2 + \frac{1}{7}x - \frac{5}{7},$$

it follows that

$$|T_g(\theta_1)| = 1,\ |T_g(\theta_2)| = |T_g(\theta_3)| = |T_g(\theta_4)| = \frac{5}{7},$$

and

$$\left(\min_{1 \leqslant i \leqslant 4} |T_g(\theta_i)|\right)^{-1} = \frac{7}{5} \leqslant |B_0^*|^{-1} = 2.$$



# Chapter 6
# Fully Homomorphic Encryption


In 1978, Rivest et al. (1978) proposed the concepts of data bank and fully homomorphic encryption. Some individuals and organizations encrypt the original data and store them in the data bank for privacy protection. Data bank is also called data cloud. Therefore, the cloud stores a large amount of original data, which is obviously a huge wealth. How to use these data effectively? First of all, we must solve the problem of calculation of these encrypted data, which is called a privacy calculation problem. Rivest, Adleman and Dertouzos conjecture that if all data is fully homomorphic encryption, that is, the addition and multiplication of ciphertext are homomorphic to the corresponding addition and multiplication of plaintext, then the encrypted data can be effectively computed by elementary calculation without changing the structure of the plaintext data (under the condition of homomorphism). The RAD conjecture has been proposed for more than 30 years, but no one could solve this problem since the cryptographic structure of the fully homomorphic encryption system is too complicated. In 2009, C. Gentry, a computer scholar at Stanford University, first proposed a fully homomorphic encryption scheme in Gentry (2009b) based on ideal lattice, for which he won the 2022 highest award in theoretical computer science—the Godel Award. Based on Gentry's work, the second and third fully homomorphic encryption schemes based on LWE distribution and trapdoor matrix technology have also been proposed; see Brakerski and Vaikuntanathan (2011a), (2011b), (2012), (2014), (2015) and Gentry et al. (2013) in 2013. The main purpose of this chapter is to systematically analyze and discuss the above three fully homomorphic encryption techniques, in order to understand the latest research trends of the post-quantum cryptography.



Z. Zheng et al., *Modern Cryptography Volume 2*, Financial Mathematics and Fintech,
https://doi.org/10.1007/978-981-19-7644-5_6

## 6.1 Definitions and Examples

Let $R_1$ be the plaintext space, $R_2$ be the ciphertext space, $R$ be the keyspace. For $s \in R$,

$$R_1 \xrightarrow{f_s} R_2 \xrightarrow{f_s^{-1}} R_1,\ s \in R,$$

we call $f_s$ the encryption function under the key $s$, and $f_s^{-1}$ is called the decryption function. In mathematical cryptosystem, $f_s$ is injective so that $f_s^{-1}$ is the left inverse mapping of $f_s$, i.e. $f_s^{-1} f_s = 1_{R_1}$, which guarantees decrypting plaintext successfully with probability 100%. However, in probabilistic cryptosystem, $f_s$ is not an injective mapping, while the probability of $f_s^{-1}$ being a left inverse mapping should be close enough to 1, i.e.

$$\Pr\{f_s^{-1} f_s = 1_{R_1}\} \geqslant 1 - \delta,\ \forall \delta > 0.$$

Hash function is a classic probabilistic cryptosystem. The phenomenon that two plaintexts are encrypted into the same ciphertext, in other words, one ciphertext could be decrypted into two plaintexts, is called a collision. If the probability of collision is small enough, then it is called an anti-collision Hash function. The cryptosystem constructed by the anti-collision Hash function is the mainstream algorithm of probabilistic cryptography. No matter mathematical or probabilistic cryptosystem, we treat the decryption transformation $f_s^{-1}$ as the left inverse mapping of $f_s$, but it is only an equality with high probability.

**Definition 6.1.1** Let $R_1 \xrightarrow{f_s} R_2 \xrightarrow{f_s^{-1}} R_1$, $R$ be the keyspace, $s \in R$, suppose $R_1$ and $R_2$ are additive groups.

1. If there is $s \in R$ such that

$$f_s^{-1}(c_1 + c_2) = f_s^{-1}(c_1) + f_s^{-1}(c_2),\ \forall c_1, c_2 \in R_2, \tag{6.1.1}$$

   we call $f_s$ the additive homomorphic encryption function.
2. If 'multiplication' is defined in $R_1$ and $R_2$, and there is $s \in R$ such that

$$f_{s^*}^{-1}(c_1 c_2) = f_s^{-1}(c_1) \cdot f_s^{-1}(c_2),\ \forall c_1, c_2 \in R_2, \tag{6.1.2}$$

   we call $f_s$ the multiplicative homomorphic encryption function, where $s^*$ is the corresponding key of $s$ under multiplication.
3. If $f_s$ is both additive and multiplicative homomorphic encryption function, then $f_s$ is called the fully homomorphic encryption function.

***Remark 6.1.1*** The multiplication defined in the ciphertext space $R_2$ is not closed, i.e. there are $c_1, c_2 \in R_2$, $c_1 c_2 \notin R_2$. We denote the result of the multiplication as $R_2 \otimes R_2$, i.e.

$$\forall c_1, c_2 \in R_2 \Rightarrow c_1 \cdot c_2 \in R_2 \otimes R_2,$$

then the corresponding key in $R_2 \otimes R_2$ is $s^* = s \otimes s$.

***Remark 6.1.2*** By (6.1.1), $f_s^{-1}(c_1 + c_2)$ is the plaintext $u$ corresponding to the ciphertext $c_1 + c_2$, $f_s^{-1}(c_1)$ and $f_s^{-1}(c_2)$ are the plaintexts $u_1$, $u_2$ corresponding to the ciphertexts $c_1$ and $c_2$. (6.1.1) is equivalent to:

$$f_s^{-1}(c_1 + c_2) = u = u_1 + u_2,$$

that is, ciphertext addition is homomorphic to plaintext addition, so is multiplication homomorphism. If $f_s$ is fully homomorphic encryption, then we can perform polynomial calculations and rational function calculations on ciphertexts. By Taylor expansion, any elementary operation (exponential function, logarithmic function, trigonometric function, etc.) can be approximated by polynomials. Therefore, for fully homomorphic encrypted data $c$, we can do any elementary operation without changing the structure of the plaintext.

We give a few examples to further understand the Definition 6.1.1.

***Example 6.1*** Homogeneous Affine Hill Cryptosystem (see Chap. 4, Sect. 4.7 in Zheng 2022) is additive homomorphic encryption.

Let $q \geqslant 1$ be a positive integer, $\mathbb{Z}_q$ be the residue class ring mod $q$, $A \in \mathbb{Z}_q^{n\times n}$ be an invertible $n$ dimensional matrix. The Homogeneous Affine Hill encryption function is $f_A$: $\forall m \in \mathbb{Z}_q^n$ is a plaintext, then

$$c = f_A(m) = A \cdot m \in \mathbb{Z}_q^n,\ c \text{ is the ciphertext,}$$

it follows that $f_A^{-1}(c) = A^{-1}c = m$. For any $c_1, c_2 \in \mathbb{Z}_q^n$, we have

$$f_A^{-1}(c_1 + c_2) = A^{-1}(c_1 + c_2) = A^{-1}c_1 + A^{-1}c_2 = f_A^{-1}(c_1) + f_A^{-1}(c_2),$$

so $f_A$ is additive homomorphic encryption.

***Example 6.2*** The public key cryptography RSA (see Chap. 4, Sect. 4.7 in Zheng 2022) is multiplicative homomorphic encryption.

Let $n > 1$ be the product of two prime numbers, $\varphi(n)$ be the Euler function, $1 \leqslant e < \varphi(n)$, $(e, \varphi(n)) = 1$, $e$ be the public key, $d = e^{-1} \bmod \varphi(n)$, $1 \leqslant d < \varphi(n)$, $d$ be the private key, i.e.

$$ed \equiv 1 \ (\mathrm{mod}\ \varphi(n)),\ 1 \leqslant d < \varphi(n).$$

We define the encryption function of RSA $f_e : \mathbb{Z}_n \to \mathbb{Z}_n$ which is a one-to-one correspondence,

$$c = f_e(m) \equiv m^e \ (\mathrm{mod}\ n),\ \forall m \in \mathbb{Z}_n,$$

the decryption function is

$$f_e^{-1}(c) \equiv c^d \ (\mathrm{mod}\ n).$$

Obviously, for any two ciphertexts $c_1, c_2 \in \mathbb{Z}_n$, it follows that

$$\begin{aligned} f_e^{-1}(c_1c_2) &\equiv (c_1c_2)^d \pmod{n} \\ &\equiv c_1^d \cdot c_2^d \pmod{n} \\ &\equiv f_e^{-1}(c_1) f_e^{-1}(c_2) \pmod{n}. \end{aligned}$$

Thus, we have $f_e^{-1}(c_1c_2) = f_e^{-1}(c_1) \cdot f_e^{-1}(c_2)$ in $\mathbb{Z}_n$, and we confirm that RSA is multiplicative homomorphic encryption.

Based on Examples 6.1 and 6.2, to construct a fully homomorphic encryption system, which is essentially a ring homomorphism between two rings in algebra, let's look at the following Example 6.3 first.

***Example 6.3*** Let $R_1$ and $R_2$ be two commutative rings, encryption function $f : R_1 \to R_2$ be a single ring homomorphism. The $f$ is fully homomorphic encryption.

In fact, since $f$ is a single homomorphism and $R_1$ is the plaintext space, then $f(R_1) \subset R_2$ is a subring of $R_2$, that is, the plaintext space is embedded into the ciphertext space. Let $c_1, c_2 \in R_2$ be any two ciphertexts, there exist $u_1, u_2 \in R_1 \Rightarrow f(u_1) = c_1$, $f(u_2) = c_2$, thus,

$$\begin{aligned} f^{-1}(c_1 + c_2) &= f^{-1}(f(u_1) + f(u_2)) \\ &= f^{-1}(f(u_1 + u_2)) = u_1 + u_2 = f^{-1}(c_1) + f^{-1}(c_2). \end{aligned}$$

Similarly,

$$\begin{aligned} f^{-1}(c_1c_2) &= f^{-1}(f(u_1) \cdot f(u_2)) \\ &= f^{-1}(f(u_1u_2)) = u_1 \cdot u_2 = f^{-1}(c_1) \cdot f^{-1}(c_2). \end{aligned}$$

Hence, $f$ is fully homomorphic encryption.

Next, we use the Chinese Remainder Theorem to construct an example of fully homomorphic encryption.

***Example 6.4*** Let $N = n_1n_2 \ldots n_k$, where $\{n_i\}$ are mutually coprime positive integers. Denote the plaintext spaces $R_1$ and $R_2$ as

$$R_1 = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \cdots \oplus \mathbb{Z}_{n_k}, \ R_2 = \mathbb{Z}_n,$$

here $R_1$ is the direct sum of $k$ rings $\mathbb{Z}_{n_i}$. Let $a = (a_1, a_2, \ldots, a_k) \in R_1$ be a plaintext, based on the Chinese Remainder Theorem, there is only one $x \in \mathbb{Z}_N$ such that

$$x \equiv a_i \pmod{n_i}, \ 1 \leqslant i \leqslant k.$$

We define the encryption function $f : R_1 \to R_2$ as $f(a) = x$. Now we prove that $f$ is fully homomorphic encryption. Let $f(a) = x_1$, $f(b) = x_2$, then

$$x_1 + x_2 \equiv a_i + b_i \pmod{n_i}, \ \forall i = 1, 2, \ldots, k.$$

So we have

$$f^{-1}(x_1 + x_2) = a + b = f^{-1}(x_1) + f^{-1}(x_2).$$

Similarly,

$$x_1 x_2 \equiv a_i b_i \pmod{n_i}, \ \forall i = 1, 2, \ldots, k.$$

Therefore,

$$f^{-1}(x_1 x_2) = a \cdot b = f^{-1}(x_1) \cdot f^{-1}(x_2).$$

This means that $f$ is fully homomorphic encryption. By Chinese Remainder Theorem, the computing complexity of $x$ is $O(k\log^k N)$, we have the simplest fully homomorphic encryption in this example.

From Example 6.4, it can be seen that it is not difficult to construct symmetric fully homomorphic encryption, but the data bank envisaged by Rivest, Adleman and Dertouzos are all data encrypted by public key cryptography. So RAD conjecture is to construct an asymmetric fully homomorphic encryption system. When the encryption key and the decryption key are separated, it becomes a very difficult work to satisfy the fully homomorphic property. The work of Gentry in 2009 or later only solve part of the RAD conjecture. They can construct a fully homomorphic encryption system under a bounded condition, while under the unbounded condition, the RAD problem is still an unsolved open problem.

Fully homomorphic encryption is similar to ring homomorphism. When constructing an asymmetric fully homomorphic encryption system, because the problem is too difficult, Gentry decomposed the decryption transformation into a composite of two mappings in Gentry (2010). The fully homomorphic properties are discussed separately for each composite factor, thus forming the current technology of bounded fully homomorphic encryption.

Let $R_1 \xrightarrow{f_s} R_2 \xrightarrow{f_s^{-1}} R_1$ be a cryptosystem, assume that $R_1$ is a ring. Decompose $f_s^{-1}$ into $R_2 \xrightarrow{\sigma_1} R_3 \xrightarrow{\sigma_2} R_1$, where $R_3$ is a ring, $f_s^{-1} = \sigma_2 \circ \sigma_1$. If both $\sigma_1$ and $\sigma_2$ are homomorphism of rings, then

$$f_s^{-1}(c_1 + c_2) = \sigma_2(\sigma_1(c_1 + c_2)) = \sigma_2(\sigma_1(c_1) + \sigma_1(c_2))$$

$$= \sigma_2\sigma_1(c_1) + \sigma_2\sigma_1(c_2) = f_s^{-1}(c_1) + f_s^{-1}(c_2).$$

**Definition 6.1.2** Under the above assumptions, if there is a set $M$ such that

1. If $f_s^{-1}(c_1) + f_s^{-1}(c_2) \in M \cap R_3$, then

$$f_s^{-1}(c_1 + c_2) = f_s^{-1}(c_1) + f_s^{-1}(c_2).$$

2. If $f_s^{-1}(c_1) \cdot f_s^{-1}(c_2) \in M \cap R_3$, then

$$f_{s^*}^{-1}(c_1 c_2) = f_s^{-1}(c_1) f_s^{-1}(c_2).$$

Generally, a bounded fully homomorphic can only perform a finite number of homomorphic calculations. Because after repeated addition and multiplication of the ciphertext, the corresponding plaintext may run out of the boundary, so the homomorphic property cannot be guaranteed.

## 6.2 Gadget Matrix and Gadget Technique

Gadget technique is developed from the work of Ajtai in 1999 (Ajtai, 1999), see Agrawal et al. (2010), Alperin-Sheriff and Peikert (2013), Alwen and Peikert (2009), Peikert and Waters (2008) and which plays an important role in bounded fully homomorphic encryption. To better understand gadget matrix and gadget technique, we start with the classical short integer solution problem (SIS).

Let $A \in \mathbb{Z}_q^{n\times m}$ be a given $n \times m$ dimensional matrix, $u \in \mathbb{Z}_q^n$ be the target vector. Find the shortest integer vector $x \in \mathbb{Z}_q^m$ such that

$$Ax \equiv u \ (\mathrm{mod}\ q),\ |x| \leqslant \beta. \tag{6.2.1}$$

The shortest integer solution $x$ in (6.2.1) is actually the shortest vector in the following $q$ ary lattice

$$L_u^{\perp}(A) = \{x \in \mathbb{Z}_q^m \mid Ax \equiv u \ (\mathrm{mod}\ q)\} \cup q\mathbb{Z}_q^m, \tag{6.2.2}$$

which is the general form of the SIS problem. If $u = 0$, the above problem becomes the classic SIS problem. For general matrix $A$, the SIS problem is difficult, but for some special matrices, such as the gadget matrix we will introduce later, the exact shortest integer solution is easy to find.

We begin from $n = 1$, if $A$ is an $l$ dimensional row vector ($1 \times l$ dimensional matrix), where $l = \lfloor \log_2 q \rceil$, i.e. $l$ is the largest integer such that $2^{l-1} \leqslant q < 2^l$, let

$$g = \begin{pmatrix} 1 \\ 2 \\ 4 \\ \vdots \\ 2^{l-1} \end{pmatrix} \in \mathbb{Z}_q^l. \tag{6.2.3}$$

**Lemma 6.2.1** *Let $A = g'$ be an $l$ dimensional vector, then the shortest vector in the $q$ ary lattice $L_u^{\perp}(g')$ could be accurately calculated. Suppose the binary representation of $u \in \mathbb{Z}_q$ is*

$$u = (a_0 a_1 \ldots a_{l-1})_2 \Rightarrow \alpha = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{l-1} \end{pmatrix} \in L_u^{\perp}(g') \tag{6.2.4}$$

*is the shortest vector. In other words, the smallest integer solution of* $g'x \equiv u \ (mod\ q)$ *is* $x = \alpha$.

***Proof*** $u \in \mathbb{Z}_q$, $0 \leqslant u < q$, since $2^{l-1} \leqslant q < 2^l$, $u$ could be represented as

$$u = a_0 + a_1 \cdot 2 + \cdots + a_{l-1} 2^{l-1},\ a_i = 0 \text{ or } 1.$$

Based on the definition of $g$ in (6.2.3) and the definition of $\alpha$ in (6.2.4), we have $g'\alpha = u$, it follows that $\alpha$ is the smallest integer solution of $g'x \equiv 0 \ (\mathrm{mod}\ q)$. Lemma 2.1 holds. □

The gadget vector defined by (6.2.3) can also be used as a sample of the one dimensional LWE distribution, so that the solution of the LWE distribution can be easily solved. Let $A = g' \in \mathbb{Z}_q^{1\times l}$, $b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_l \end{pmatrix} \in \mathbb{Z}_q^l$, we get the $\mathrm{LWE}_{1,q,\chi,l}$ problem (see Definition 3.3.3 in Chap. 3)

$$b_i \equiv_\chi 2^i s_i + e_i \ (\mathrm{mod}\ q),\ e = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_l \end{pmatrix} \leftarrow \chi^l,\ 1 \leqslant i \leqslant l.$$

If the LWE distribution $A_{s,\chi} = (i, b)$ is given, we can get the following relations with high probability

$$s_i \equiv_\chi 2^{-i} b_i \ (\mathrm{mod}\ q),\ 1 \leqslant i \leqslant l.$$

In order to generalize the above gadget technique to high dimensions, i.e. $n > 1$, we need to replace the gadget vector $g$ defined in (6.2.3) with the gadget matrix. Let $A = (a_{ij})_{n_1\times n_2}$, $B = (b_{ij})_{m_1\times m_2}$, the Kronecker product $A \otimes B$ (see Chap. 2 in Zheng 2022) of the matrices $A$ and $B$ is defined as

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n_2}B \\ a_{21}B & a_{22}B & \cdots & a_{2n_2}B \\ \vdots & \vdots & & \vdots \\ a_{n_1 1}B & a_{n_1 2}B & \cdots & a_{n_1 n_2}B \end{pmatrix}_{n_1 m_1 \times n_2 m_2}. \tag{6.2.5}$$

**Definition 6.2.1** Assume $n > 1$, $I_n$ is the $n$ dimensional identity matrix. We define the $n \times nl$ dimensional gadget matrix $G$ as the following block diagonal matrix,

$$G = I_n \otimes g' = \text{diag}\{g', g', \ldots, g'\} \in \mathbb{Z}_q^{n \times nl}, \tag{6.2.6}$$

where $g$ is the gadget vector defined in (6.2.3).

**Lemma 6.2.2** *Let $G$ be a gadget matrix, $u \in \mathbb{Z}_q^{nl}$ be the target vector. Then the shortest integer solution $x \in \mathbb{Z}_q^{nl}$ of the SIS problem $Gx \equiv u \pmod q$ could be uniquely determined by lemma 2.1.*

***Proof*** Let $u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \in \mathbb{Z}_q^n$ be a given target vector, $x$ be an $nl$ dimensional column vector divided into

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \text{ where } x_i \in \mathbb{Z}^l, \ 1 \leqslant i \leqslant n.$$

Based on the definition of gadget matrix $G$, the SIS problem $Gx \equiv u \pmod q$ is equivalent to the following $n$ equations:

$$g' x_i \equiv u_i \pmod q, \ 1 \leqslant i \leqslant n.$$

By lemma 2.1, the shortest integer solution of each equation could be uniquely determined as $x_i = \alpha_i \in \mathbb{Z}^l$, so $x = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$ is the shortest integer solution of $Gx \equiv u \pmod q$. □

**Definition 6.2.2** For any $u \in \mathbb{Z}_q^n$, we define function: $\mathbb{Z}_q^n \xrightarrow{G^{-1}} \mathbb{Z}^{nl}$ as $G^{-1}(u) = x$, where $x \in \mathbb{Z}^{nl}$ is the shortest integer solution of $Gx \equiv u \pmod q$.

Lemma 6.2.2 guarantees the existence of the function $G^{-1}$ and gives the way to compute the vector $x$. By Definition 6.2.2, we have

$$GG^{-1}(u) \equiv u \pmod q, \tag{6.2.7}$$

the above function $G^{-1} : \mathbb{Z}_q^n \to \mathbb{Z}^{nl}$ could be regarded as the 'inverse' matrix of the gadget matrix $G$.

When using the gadget matrix $G$ as the LWE distribution sample to solve the LWE problem, notice that for any $n$ dimensional vector $s = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \in \mathbb{Z}_q^n$, we have

$$s'G = (s_1 g', s_2 g', \ldots, s_n g') \in \mathbb{Z}_q^{nl}. \tag{6.2.8}$$

For the LWE distribution $A_{s,\chi} = (G, b)$, where $b \in \mathbb{Z}_q^{nl}$, to solve the private key $s$,

$$b' = s'G, \quad b \in \mathbb{Z}_q^{nl}, \quad s \in \mathbb{Z}_q^n,$$

based on (6.2.8), it can be transformed into $n$ one dimensional LWE distribution problems, which has been discussed above.

The solutions of the SIS problem and the LWE problem discussed above are easy to compute because these problems are based on specific gadget vectors and gadget matrices. To get more general results, we need the trapdoor matrix, the tag matrix (tag) and the Gauss matrix. An integer matrix $R$ is called a Gauss matrix, if all of its components are independent and have the discrete Gauss distribution. Since the Gauss distribution has the greatest probability near 0, a random Gauss matrix is also called a short integer vector matrix in the sense of high probability.

**Definition 6.2.3** Let $A \in \mathbb{Z}_q^{n\times m}$ be a given matrix, $R \in \mathbb{Z}^{m\times nl}$ be a Gauss matrix, $H \in \mathbb{Z}_q^{n\times n}$ be an invertible $n$ dimensional square matrix, $G \in \mathbb{Z}_q^{n\times nl}$ be a gadget matrix, if

$$AR \equiv HG \pmod q, \tag{6.2.9}$$

then we call $R$ as the trapdoor matrix of $A$, and $H$ is the tag matrix.

Generally, $A$ is called the check matrix, and $R$ satisfying (6.2.9) is called the trapdoor matrix of the check matrix $A$ with the tag $H$. To better understand the Definition 6.2.2, by Lemma 6.2.2, the SIS problem generated by the gadget matrix $G$ can be easily calculated. If $H \in \mathbb{Z}_q^{n\times n}$ is an invertible matrix, then the SIS or LWE problems generated by $HG$ are also easy to compute. In fact, for any target vector $u \in \mathbb{Z}_q^{n\times n}$,

$$HGx \equiv u \pmod q \Leftrightarrow Gx \equiv H^{-1}u \pmod q.$$

The shortest integer solution of the SIS problem in the right hand is $G^{-1}(H^{-1}u)$; therefore, the shortest integer solution of $HGx \equiv u \pmod q$ is $x = G^{-1}(H^{-1}u)$, where the target vector is replaced by $H^{-1}u$. We can discuss the LWE problem generated by $HG$ in the same way. Next we generalize the results to a general matrix $A$.

**Lemma 6.2.3** *For any check matrix $A \in \mathbb{Z}_q^{n\times m}$, the shortest integer solution of the SIS problem $Ax \equiv u \pmod q$ generated by $A$ could be approximated as*

$$x = Rw, \quad where\ w = G^{-1}(H^{-1}u), \tag{6.2.10}$$

*$R$ is the trapdoor matrix of $A$ with tag $H$.*

***Proof*** If the trapdoor matrix $R$ of $A$ exists, let $x = Rw$ in the SIS problem $Ax \equiv u \pmod q$ ($x \in \mathbb{Z}^m$, the target vector $u \in \mathbb{Z}_q^n$) generated by $A$, where $w \in \mathbb{Z}^{nl}$, therefore,

$$Ax \equiv u \pmod q \Rightarrow ARw \equiv u \pmod q,$$

we have

$$HGw \equiv u \pmod q \Rightarrow w = G^{-1}(H^{-1}u). \tag{6.2.11}$$

Since $w$ is the shortest integer solution of (6.2.11), and the trapdoor matrix $R$ is a Gauss matrix, so $x = Rw = RG^{-1}(H^{-1}u)$ is a short integer solution of the SIS problem generated by $A$, i.e. we can regard $RG^{-1}(H^{-1}u)$ as an approximation of the SIS problem. □

To quantify the efficiency of the approximation of (6.2.10), we define the mass $s_1(R)$ of the trapdoor matrix $R$

$$s_1(R) = \max_{z \in \mathbb{Z}^{nl}, |z|=1} |Rz|. \tag{6.2.12}$$

By (6.2.10),

$$|x| = |Rw| \leqslant s_1(R)|w|, \tag{6.2.13}$$

thus, the smaller $s_1(R)$ is, the shorter $|x|$ is, and the approximation of the solution of the SIS problem is more accurate. So we can say that the smaller $s_1(R)$, the higher mass of the trapdoor matrix $R$.

Finally, let's discuss the generation of trapdoor matrix. For any uniformly distributed random matrix $\overline{A} \in \mathbb{Z}_q^{n \times \overline{m}}$, suppose $\overline{R} \in \mathbb{Z}_q^{\overline{m} \times nl}$ is a Gauss matrix, let

$$A = [\overline{A}, HG - \overline{A}\,\overline{R}] \in \mathbb{Z}_q^{n \times m},\ m = \overline{m} + nl, \tag{6.2.14}$$

where $H \in \mathbb{Z}_q^{n \times n}$ is a given invertible matrix, $G$ is the gadget matrix.

**Lemma 6.2.4** *If $A$ is given by (6.2.14), then the trapdoor matrix of $A$ with the tag $H$ is*

$$R = \begin{pmatrix} \overline{R} \\ I_n \end{pmatrix} \in \mathbb{Z}_q^{m \times nl},\ m = \overline{m} + nl. \tag{6.2.15}$$

***Proof*** From the definition of $A$ and $R$

$$AR = [\overline{A}, HG - \overline{A}\,\overline{R}] \begin{pmatrix} \overline{R} \\ I_n \end{pmatrix}$$

$$\equiv \overline{A}\,\overline{R} + HG - \overline{A}\,\overline{R} \pmod{q}$$

$$\equiv HG \pmod{q},$$

so the trapdoor matrix of $A$ with the tag $H$ is $\begin{pmatrix}\overline{R}\\ I_n\end{pmatrix}$. □

The mass $s_1(R)$ of the Gauss matrix $R$ can be estimated using classical random matrix theory. The following result is referred from R.Vershynin's monograph 'Compressed Sensing, Theory and Applications' Chap. 5, p. 210–268, Cambridge University Press, 2012.

**Lemma 6.2.5** *Suppose* $R = \begin{pmatrix}\overline{R}\\ I_n\end{pmatrix}$ *is given by (6.2.15),* $\overline{R}$ *is a Gauss matrix with parameter s in the Gauss distribution. Then we have the following relation with high probability*

$$s_1(R) = O(s(\sqrt{\overline{m}} + \sqrt{nl})).$$

***Proof*** Based on the definition of trapdoor matrix,

$$s_1(R) = \max_{z\in\mathbb{Z}^{nl},|z|=1} |Rz| = \max_{z\in\mathbb{Z}^{nl},|z|=1} \left|\begin{pmatrix}\overline{R}\\ I_n\end{pmatrix} z\right|$$

$$= \max_{z\in\mathbb{Z}^{nl},|z|=1} \left|\begin{pmatrix}\overline{R}z\\ z\end{pmatrix}\right| = \max_{z\in\mathbb{Z}^{nl},|z|=1} \sqrt{|\overline{R}z|^2 + |z|^2},$$

denote $\overline{R} = (r_{ij})_{\overline{m}\times nl}$, where $r_{ij}$ has the discrete Gauss distribution with parameter $s$. By Chebyshev inequality, for any positive integer $k$,

$$\Pr\{|r_{ij}| \leqslant ks\} \geqslant 1 - \frac{\mathrm{Var}(r_{ij})}{k^2s^2} \geqslant 1 - \frac{s^2}{2\pi k^2 s^2} = 1 - \frac{1}{2\pi k^2}.$$

It follows that the probability of all the $\overline{m}\cdot nl$ variables $r_{ij}$ satisfying $|r_{ij}| \leqslant ks$ is at least $(1 - \frac{1}{2\pi k^2})^{\overline{m}nl}$. We choose $k$ large enough so that this probability is sufficiently close to 1, thus,

$$s_1(R) = \max_{z\in\mathbb{Z}^{nl},|z|=1} \sqrt{|\overline{R}z|^2 + |z|^2} \leqslant \sqrt{\sum_{i=1}^{\overline{m}}\sum_{j=1}^{nl} r_{ij}^2 + 1}$$

$$\leqslant \sqrt{1 + \overline{m}nlk^2s^2} \leqslant Ks(\sqrt{\overline{m}} + \sqrt{nl}),$$

where $K = (k+1)\sqrt{\overline{m}nl}\,/\,(\sqrt{\overline{m}} + \sqrt{nl})$, so we have

$$Pr\{s_1(R) \leqslant Ks(\sqrt{\overline{m}} + \sqrt{nl})\} \geqslant (1 - \frac{1}{2\pi k^2})^{\overline{m}nl},$$

i.e. in the sense of high probability

$$s_1(R) = O(s(\sqrt{m} + \sqrt{nl})). \qquad \square$$

## 6.3 Bounded Fully Homomorphic Encryption

In 2009, C. Gentry of Stanford University in the USA first proposed a bounded fully homomorphic encryption based on ideal lattices, which has a great influence in the field of theoretical computer science, and a number of improved works have been proposed one after another. Brakerski and Vaikuntanathan proposed a fully homomorphic encryption system based on the LWE cryptography in 2011 (see Brakerski & Vaikuntanathan, 2011a, 2011b, 2014, 2015), which we call BV fully homomorphic encryption. Another improvement is the fully homomorphic encryption using trapdoor matrix proposed by Gentry, Sahai and Waters in 2013, which we call GSW fully homomorphic encryption. BV and GSW cryptosystems are currently the most active and cutting-edge research. The main purpose of this section is to introduce these two fully homomorphic encryption systems.

**1. BV fully homomorphic encryption**

Review the LWE cryptosystem by Regev introduced in Chap. 4. Let $n \geqslant 2$, $q \geqslant 2$, $\chi$ is a given distribution on $\mathbb{Z}_q$. The $(n-1)$ dimensional LWE distribution obtained by random sampling is (see Definition 3.3.2 in Chap. 3)

$$\begin{cases} A_{s,\chi} = (\overline{a}, b) \in \mathbb{Z}_q^{n-1} \times \mathbb{Z}_q, \\ b \equiv_\chi < \overline{a}, \overline{s} > + e \pmod{q}, \end{cases} \tag{6.3.1}$$

where $\overline{a} \in \mathbb{Z}_q^{n-1}$ is uniformly distributed, $\overline{s} \in \mathbb{Z}_q^{n-1}$ is the randomly chosen private key, $e \in \mathbb{Z}_q$ has the distribution $\chi$. Generally, $\chi$ is chosen as the discrete Gauss distribution on $\mathbb{Z}_q$. Let

$$a = \begin{pmatrix} \overline{a} \\ b \end{pmatrix} \in \mathbb{Z}_q^n, \quad s = \begin{pmatrix} -\overline{s} \\ 1 \end{pmatrix} \in \mathbb{Z}_q^n,$$

$a$ is the public key and $s$ is the private key. The key equality of the LWE cryptosystem $(m = 1)$ encryption and decryption algorithm is:

$$\begin{aligned} <a, s> &= (-\overline{s}', 1) \begin{pmatrix} \overline{a} \\ b \end{pmatrix} \\ &= b - <\overline{a}, \overline{s}> \equiv_\chi e \pmod{q}, \end{aligned} \tag{6.3.2}$$

$e \in \mathbb{Z}_q$ has the discrete Gauss distribution, and $e$ is very close to 0 with high probability, so it is also called the error term.

To better understand the fully homomorphic encryption technology based on the above LWE cryptosystem, we rewrite it into the form of symmetric encryption by formula (6.3.2).

**Most significant bit**

Let $s \in \mathbb{Z}_q^n$ be a private key, $q > 2$ be an odd number, $u \in \mathbb{Z}_2$ be the plaintext. The most significant bit of plaintext $u$ by the LWE distribution $A$ is $c = f_A(u)$, where $c \in \mathbb{Z}_q^n$ is the ciphertext, satisfying

$$<s, c> \equiv_\chi u \left\lfloor \frac{q}{2} \right\rceil \pmod q, \ c \in \mathbb{Z}_q^n, \tag{6.3.3}$$

where $<s, c>$ is inner product. Equation (6.3.3) is not an exact congruence equation, but a congruence equation with error which has small probability. It should be noted that the encryption function $f_A$ is only formal, and its specific algorithm depends on the samples of the LWE distribution (see Chap. 4).

Using the private key $s \in \mathbb{Z}_q^n$, the decryption of the ciphertext $c$ is defined by

$$\begin{aligned} f_A^{-1}(c) &\equiv_\chi \left\lfloor \frac{2}{q} <s, c> \right\rceil \pmod q \\ &\equiv_\chi \left\lfloor \frac{2}{q} \lfloor \frac{q}{2} u \right\rceil \rceil \pmod q \\ &\equiv_\chi u \pmod q \text{ (see Lemma 3.3 in Chap. 4).} \end{aligned} \tag{6.3.4}$$

In order to better understand the fully homomorphic property (bounded) of the LWE cryptosystem, we write the most significant bit as the following equivalent least significant bit.

**Least significant bit**

Assume $q > 2$ is an odd number, let $m \equiv u \pmod 2$, and $-\frac{q}{2} < m \leqslant \frac{q}{2}$, $u$ be a given plaintext $u \in \mathbb{Z}_2$, i.e.

$$m \in \{u + 2\mathbb{Z}\} \cap \big( -\frac{q}{2}, \frac{q}{2} \big]. \tag{6.3.5}$$

The least significant bit of $u$ is $f_A(u) = c \in \mathbb{Z}_q^n$, where the ciphertext $c$ satisfies

$$<s, c> \equiv m \pmod q, \tag{6.3.6}$$

(6.3.6) is an exact congruence equation.

The decryption of the ciphertext $c$ still uses the private key $s \in \mathbb{Z}_q^n$, which is divided into the following two steps:

1. There exists only one $m$ satisfying $m \equiv <s, c> \pmod q$, and $-\frac{q}{2} \leqslant m < \frac{q}{2}$.
2. $u \equiv m \pmod 2$, then we get the plaintext $f_A^{-1}(c) = u$.

We will prove that the most significant bit and the least significant bit are actually equivalent for multibit plaintext in the general case. First, we look at the difference between the two encryptions in the case of $u \in \mathbb{Z}_2$. Write Eq. (6.3.3) in the error form,

$$<s, c> \equiv e + u \left\lfloor \frac{q}{2} \right\rceil \pmod{q},$$

then

$$f_A^{-1}(c) \equiv \left\lfloor \frac{2}{q} e \right\rceil + u \pmod{q}.$$

For a real number $x$, $\lfloor x \rceil = 0 \Leftrightarrow -\frac{1}{2} < x \leqslant \frac{1}{2}$, so $-\frac{q}{4} < e \leqslant \frac{q}{4}$. Compared with (4.1.7) in Chap. 4, the decryption of the Regev's cryptosystem is actually Eq. (6.3.4) here. This observation enables us to construct corresponding cryptosystem for multibit plaintext.

Let $1 < p < q$ be two positive integers, $(p, q) = 1$, $\mathbb{Z}_p$ be the plaintext space, $\mathbb{Z}_q^n$ be the ciphertext, $s \in \mathbb{Z}_q^n$ be the randomly chosen private key.

Most significant bit: for a given plaintext $u \in \mathbb{Z}_p$, we define the most significant bit of $u$ as $M(u) = w \in \mathbb{Z}_q$ satisfying

$$\left\lfloor \frac{p}{q} w \right\rceil \equiv u \pmod{p}, \tag{6.3.7}$$

in fact, based on $w = <s, c>$, we can write the ciphertext as,

$$M(u) = w \equiv \left\lfloor \frac{q}{p} u \right\rceil \pmod{q}, \tag{6.3.8}$$

the decryption function

$$M^{-1}(w) \equiv \left\lfloor \frac{p}{q} w \right\rceil \equiv u \pmod{p},$$

we can get the plaintext $u$.

Least significant bit: the least significant bit for a given plaintext $u \in \mathbb{Z}_p$ is $v$, i.e. $L(u) = v \in \mathbb{Z}_q$ satisfies

$$v \equiv e \pmod{q},\ e \equiv u \pmod{p},\ -\frac{q}{2} \leqslant e < \frac{q}{2},$$

the decryption for the ciphertext $v$: there exists only one $e \in [-\frac{q}{2}, \frac{q}{2}) \Rightarrow v \equiv e \pmod{q}$, let $u \equiv e \pmod{p}$, then $M^{-1}(v) = u$. In fact the $v$ here is $<s, c>$.

**Lemma 6.3.1** *If $1 < p < q$, $(p, q) = 1$, then the most significant bit and the least significant bit are equivalent.*

***Proof*** Since $(p, q) = 1$, then there are integers $c_p \in \mathbb{Z}$, $c_q \in \mathbb{Z} \Rightarrow$

$$c_p \cdot p + c_q \cdot q = 1.$$

Actually $c_p$ is the multiplicative inverse of $p$ under mod $q$, $c_q$ is the multiplicative inverse of $q$ under mod $p$. Denote $c_p = p^{-1}$ and $c_q = q^{-1}$.

Assume $v \in \mathbb{Z}_q$ is the least significant bit of the plaintext $u \in \mathbb{Z}_p$, i.e. $L(u) = v$. We are to prove that the most significant bit of the plaintext $-q^{-1}u \in \mathbb{Z}_p$ is $p^{-1}v \in \mathbb{Z}_q$, i.e.

$$M(-q^{-1}u) = p^{-1}v.$$

Based on $v \equiv e \pmod q$, $e \in \{u + p\mathbb{Z}\} \cap [-\frac{q}{2}, \frac{q}{2})$, so we have

$$\begin{aligned}\left\lfloor \frac{p}{q} p^{-1} v \right\rceil &= \left\lfloor \frac{p}{q} e \frac{1 - c_q q}{p} \right\rceil \\ &= \left\lfloor \frac{e}{q} - e c_q \right\rceil \\ &= -c_q e \equiv -q^{-1}u \pmod p,\end{aligned}$$

this means $M(-q^{-1}u) = p^{-1}v$. On the other hand, if $w = M(u)$, i.e. $w$ is the most significant bit of the plaintext $u$, we confirm that the least significant bit of $-qu$ is just $pw \in \mathbb{Z}_q$, i.e.

$$L(-qu) = pw \in \mathbb{Z}_q,$$

by the definition of the most significant bit,

$$\left\lfloor \frac{p}{q} w \right\rceil = \frac{p}{q} w - r \equiv u \pmod p,$$

where $-\frac{1}{2} \leqslant r < \frac{1}{2}$, so (since $(p, q) = 1$)

$$pw - qr \equiv qu \pmod p.$$

Let $qr = e$, we get

$$pw - e \equiv qu \pmod{pq},\ -\frac{q}{2} \leqslant e < \frac{q}{2},$$

it follows that $pw \equiv e \pmod q$, and $e \equiv -qu \pmod p$, namely $L(-qu) = pw$.

Above all, there is a one-to-one correspondence between the most significant bit and the least significant bit for a plaintext, so the two forms of encryption are equivalent. □

Finally, we discuss the fully homomorphic property of the BV encryption system, which is summarized in the following theorem.

**Theorem 6.3.1** *Let $p = 2$, $q > 2$ be an odd number, then the BV encryption system is bounded fully homomorphic encryption, and its fully homomorphic boundary is*

$$M = \left(-\frac{q}{2}, \frac{q}{2}\right].$$

***Proof*** Based on the least significant bit of the BV encryption system, its decryption function $f_s^{-1}$ can be divided into two parts: $R_3 = \mathbb{Z}_q$, $\mathbb{Z}_q \xrightarrow{\sigma_2} \mathbb{Z}_2 = R_1$ is natural homomorphism, then $f_s^{-1}$ could be decomposed into

$$\mathbb{Z}_q^n \xrightarrow{\sigma_1} M \cap \mathbb{Z}_q \xrightarrow{\sigma_2} \mathbb{Z}_2,$$

where $\sigma_1$ is defined for any ciphertext $c \in \mathbb{Z}_q^n$, $c \xrightarrow{\sigma_1} m \in M \cap \mathbb{Z}_q$ satisfying

$$<s, c> \equiv m \pmod{q}.$$

Since there exists only one $m$ satisfying the above formula, $\sigma_1$ is well-defined. It follows that

$$\begin{aligned} <s, c_1 + c_2> &= < s, c_1 > + < s, c_2> \\ &\equiv m_1 + m_2 \pmod{q}, \end{aligned} \tag{6.3.9}$$

i.e. $\sigma_1(c_1 + c_2) = m_1 + m_2$, if $m_1 + m_2 \in M \cap \mathbb{Z}_q$, then

$$\begin{aligned} f_s^{-1}(c_1 + c_2) &= \sigma_2(\sigma_1(c_1) + \sigma_1(c_2)) \\ &= \sigma_2(m_1 + m_2) \\ &\equiv u_1 + u_2 \pmod{2}, \end{aligned}$$

so we have

$$f_s^{-1}(c_1 + c_2) = u_1 + u_2 = f_s^{-1}(c_1) + f_s^{-1}(c_2),$$

$f_s$ is additive fully homomorphic encryption.

To introduce the multiplicative homomorphism, we define the Kronecker convolution for two vectors in $\mathbb{Z}_q^n$. Let $c_1 = (c_{11}, c_{12}, \ldots, c_{1n}) \in \mathbb{Z}_q^n$, $c_2 = (c_{21}, c_{22}, \ldots, c_{2n}) \in \mathbb{Z}_q^n$ be two row vectors, we define the Kronecker convolution of $c_1$ and $c_2$ as $c_1 \otimes c_2$,

$$c_1 \otimes c_2 = (c_{1i} \cdot c_{2j})_{1 \leqslant i, j \leqslant n} \in \mathbb{Z}_q^{n^2}. \tag{6.3.10}$$

Obviously, for any four vectors $a, b, c, d \in \mathbb{Z}_q^n$, we have

$$<a \otimes b, c \otimes d> = <a, c> \cdot <b, d>. \tag{6.3.11}$$

In fact, let $a = (a_1, a_2, \ldots, a_n)$, $b = (b_1, b_2, \ldots, b_n)$, $c = (c_1, c_2, \ldots, c_n)$, $d = (d_1, d_2, \ldots, d_n)$, by (6.3.10),

$$\begin{aligned} <a \otimes b, c \otimes d> &= \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j c_i d_j \\ &= \left( \sum_{i=1}^{n} a_i c_i )( \sum_{j=1}^{n} b_j d_j \right) \\ &= <a, c> \cdot <b, d>, \end{aligned}$$

thus, (6.3.11) holds.

Let $c_1, c_2 \in \mathbb{Z}_q^n$ be two ciphertexts, $s \in \mathbb{Z}_q^n$ be the private key, we define the multiplication as Kronecker convolution in the ciphertext space $\mathbb{Z}_q^n$. Suppose $s^* = s \otimes s$, then the decryption function $f_{s^*}^{-1}$ is a mapping of $\mathbb{Z}_q^{n^2} \to \mathbb{Z}_2$. Based on (6.3.11), we have

$$\begin{aligned} <s \otimes s, c_1 \otimes c_2> &= <s, c_1> \cdot <s, c_2> \\ &\equiv m_1 \cdot m_2 \pmod{q}. \end{aligned}$$

If $m_1 m_2 \in M \cap \mathbb{Z}_q$, then

$$m_1 \equiv u_1 \pmod 2,\ m_2 \equiv u_2 \pmod 2 \Rightarrow m_1 m_2 \equiv u_1 u_2 \pmod 2,$$

namely

$$f_{s^*}^{-1}(c_1 \otimes c_2) = f_s^{-1}(c_1) \cdot f_s^{-1}(c_2),$$

i.e. $f_s$ satisfies the multiplicative homomorphism. So we prove the bounded fully homomorphic property of the BV encryption system, and its fully homomorphic boundary is $M = (-\frac{q}{2}, \frac{q}{2}]$. □

The above Theorem 6.3.1 can be generalized to the multibit case, that is, plaintext $u \in \mathbb{Z}_p$, ciphertext $c \in \mathbb{Z}_q^n$, $(p, q) = 1$. Under these assumptions, the BV multibit fully homomorphic encryption system can be constructed, and we leave it as a question for the readers. Note that the dimensions of the ciphertext space and key space grow from $n$ to $n^2$ by the Kronecker convolution. The dimension could be reduced by using the gadget technique in Sect. 6.2. This reduction technique is called key conversion.

**Key conversion**

Let $c_{\text{in}} = c_1 \otimes c_2$ be an $n_{\text{in}}$ dimensional ciphertext, where $c_{\text{in}}$ and $n_{\text{in}}$ represent the input ciphertext and the dimension of the ciphertext. By the most significant bit of BV fully homomorphic encryption, then

$$<s_{\text{in}}, c_{\text{in}}> = s'_{\text{in}} \cdot c_{\text{in}} \equiv_{\chi} u \left\lfloor \frac{q}{2} \right\rceil \pmod{q}. \tag{6.3.12}$$

The above formula is obtained from (6.3.3), where $s_{\text{in}}$ is the private key with dimension $n_{\text{in}}$. In order to reduce the dimension $n_{\text{in}}$, we construct a private key $s_{\text{out}}$ with lower dimension and convert the input ciphertext $c_{\text{in}}$ into the output ciphertext $c_{\text{out}}$ encrypted by $s_{\text{out}}$. Of course, the dimension $n_{\text{out}}$ of the output ciphertext $c_{\text{out}}$ and the key $s_{\text{out}}$ is much smaller than the input dimension $n_{\text{in}}$. To do this, let $G$ be the gadget matrix,

$$G = I_{n_{\text{in}}} \otimes c'_{\text{in}} = \text{diag}\{c'_{\text{in}}, c'_{\text{in}}, \ldots, c'_{\text{in}}\}_{n_{\text{in}} \times n_{\text{in}}^2}. \tag{6.3.13}$$

$G$ is the $n_{\text{in}} \times n_{\text{in}}^2$ gadget matrix generated by the $n_{\text{in}}$ dimensional vector $c_{\text{in}}$. By (6.2.7) and (6.3.12), we have

$$<s_{\text{in}}, c_{\text{in}}> = s'_{\text{in}} \cdot c_{\text{in}} \equiv (s'_{\text{in}} G) \cdot G^{-1}(c_{\text{in}}) \equiv_{\chi} u \left\lfloor \frac{q}{2} \right\rceil \pmod{q}, \tag{6.3.14}$$

where $G^{-1}(c_{\text{in}}) = x$ is the shortest integer solution of $Gx \equiv c_{\text{in}} \pmod{q}$. Based on (6.2.8), $s'_{\text{in}} \cdot G$ is an $n_{\text{in}}^2$ dimensional vector.

**Lemma 6.3.2** *For any $n < n_{in}$, then there exist a matrix $K \in \mathbb{Z}_q^{n \times n_{in}^2}$ and an $n$ dimensional private key $s_{out}$ with high probability such that*

$$s'_{out} \cdot K \equiv_{\chi} s'_{in} \cdot G \ (mod\ q). \tag{6.3.15}$$

***Proof*** The construction of the matrix $K$ and the transformed private key $s_{\text{out}}$ are related to the resampling technique (Bootstrapping) of the LWE distribution. For a given vector $b' = s'_{\text{in}} G \in \mathbb{Z}_q^{n_{\text{in}}^2}$, we can take a sample $s_{\text{out}} \in \mathbb{Z}_q^n$ for very small error distribution $e \in \mathbb{Z}_q^{n_{\text{in}}^2}$ (with high probability) and

$$A = [a_1, a_2, \ldots, a_{n_{\text{in}}}],\ \forall a_i \in \mathbb{Z}_q^n$$

satisfying (see 4.1.3 in Chap. 4)

$$(s'_{\text{out}}, -1) \begin{pmatrix} A \\ b' \end{pmatrix} \equiv_{\chi} e \pmod{q}.$$

Since $e$ is a very small error term, the above equation can be written as the form of random congruence

$$s'_{\text{out}} A \equiv_{\chi} b' = s'_{\text{in}} G \pmod{q}.$$

Let $K = A \in \mathbb{Z}_q^{n \times n_{\text{in}}^2}$, we have

$$s'_{\text{out}} K \equiv s'_{\text{in}} G \pmod{q}.$$

Lemma 6.3.2 holds. □

***Remark 6.3.1*** $K$ is the public key which could be made public, the security of the private key $s_{\text{out}}$ will not be affected based on the security of the LWE distribution.

By (6.3.14) in Lemma 6.3.2, the input ciphertext $c_{\text{in}}$ is converted into a new output ciphertext $c_{\text{out}} = KG^{-1}(c_{\text{in}})$. $c_{\text{out}}$ is obtained by using the key $s_{\text{out}}$, this is because

$$s'_{\text{out}} c_{\text{out}} = s'_{\text{out}}(KG^{-1}(c_{\text{in}}))$$

$$\equiv_\chi s'_{\text{in}} G \cdot G^{-1}(c_{\text{in}}) \equiv_\chi u \left\lfloor \frac{q}{2} \right\rceil \pmod{q}.$$

We replace $c_{\text{in}} = c_1 \otimes c_2$ and $s_{\text{in}} = s \otimes s$ with the new ciphertext $c_{\text{out}}$ and the converted key $s_{\text{out}}$, which significantly reduces the dimension of the ciphertext.

**2. GSW fully homomorphic encryption**

In 2013, Gentry et al. (2013) further improved BV fully homomorphic encryption by using gadget matrix and gadget technology. The greatest advantage is that fully homomorphic multiplication does not require the key conversion introduced in the previous subsection.

First, we select a random matrix $\overline{A} \in \mathbb{Z}_q^{n \times \overline{m}}$, with the number of columns $\overline{m}$ large enough. Define the following two matrices by $\overline{A}$

$$A_i = x_i G - \overline{A} R_i \in \mathbb{Z}_q^{n \times nl}, \ i = 1, 2, \tag{6.3.16}$$

where $x_1, x_2 \in \mathbb{Z}_q$ are two integers, $G$ is the gadget matrix,

$$G = \text{diag}\{g', g', \ldots, g'\}_{n \times nl}, \ g' \in \mathbb{Z}_q^l,$$

here $l = \lfloor \log_2 q \rceil$, $R_i \in \mathbb{Z}_q^{\overline{m} \times nl}$ is the Gauss matrix.

**Lemma 6.3.3** *1. The trapdoor matrix of* $[\overline{A}, A_1 + A_2]$ *is* $\begin{pmatrix} R_1 + R_2 \\ I_n \end{pmatrix}$, *the tag matrix is* $x_1 I_n + x_2 I_n$.

*2. The trapdoor matrix of* $[\overline{A}, A_1 G^{-1}(A_2)]$ *is* $\begin{pmatrix} R \\ I_n \end{pmatrix}$, *the tag matrix is* $x_1 x_2 I_n$, *where*

$$R = x_1 R_2 + R_1 G^{-1}(A_2). \tag{6.3.17}$$

***Proof*** By (6.3.16), it is easy to get

$$A_1 + A_2 = (x_1 + x_2)G - \overline{A}(R_1 + R_2). \tag{6.3.18}$$

We regard each column vector of $A_2$ as the target vector $u$ in Lemma 2.2, then the inverse matrix $G^{-1}$ in Definition2.2 can be generalized to $G^{-1}(A_2) \in \mathbb{Z}_q^{nl \times nl}$, here $G^{-1}(A_2) = x$ is the shortest integer solution of (because each column of the matrix $x$ is the shortest integer solution)

$$Gx \equiv A_2 \pmod{q}. \tag{6.3.19}$$

Thus, (6.2.7) generalizes to

$$G \cdot (G^{-1}(A_2)) \equiv A_2 \pmod{q}, \tag{6.3.20}$$

so we have

$$\begin{aligned} A_1 G^{-1}(A_2) &= (x_1 G - \overline{A} R_1) G^{-1}(A_2) \\ &= x_1 A_2 - \overline{A} R_1 G^{-1}(A_2) \\ &= x_1 x_2 G - x_1 \overline{A} R_2 - \overline{A} R_1 G^{-1}(A_2) \\ &= x_1 x_2 G - \overline{A}(x_1 R_2 + R_1 G^{-1}(A_2)). \end{aligned} \tag{6.3.21}$$

Let $A = [\overline{A}, A_1 + A_2]$, $R = \begin{pmatrix} R_1 + R_2 \\ I_n \end{pmatrix}$, by (6.3.18), we get

$$AR = A_1 + A_2 + \overline{A}(R_1 + R_2) = (x_1 + x_2) I_n G,$$

therefore, $R$ is the trapdoor matrix of $A$, and the tag matrix is $H = x_1 I_n + x_2 I_n$. We have proved (i) in this lemma. To prove (ii), let

$$A = [\overline{A}, A_1 G^{-1}(A_2)], \ \overline{R} = \begin{pmatrix} R \\ I_n \end{pmatrix},$$

where

$$R = x_1 R_2 + R_1 G^{-1}(A_2).$$

Based on (6.3.21),

$$\begin{aligned} A\overline{R} &= \overline{A} R + A_1 G^{-1}(A_2) \\ &= \overline{A} x_1 R_2 + \overline{A} R_1 G^{-1}(A_2) + A_1 G^{-1}(A_2) \\ &= x_1 x_2 G, \end{aligned}$$

this implies $\overline{R} = \begin{pmatrix} R \\ I_n \end{pmatrix}$ is the trapdoor matrix of $A$, and the tag matrix is $H = x_1 x_2 I_n$. So (ii) in this lemma holds. □

In order to fully prove the conclusion of lemma 3.3 , it is also necessary to prove that the corresponding trapdoor matrix is a Gauss matrix, which is summarized in the following lemma.

**Lemma 6.3.4** *If $R$ is a Gauss matrix, then $\begin{pmatrix} R \\ I_n \end{pmatrix}$ is also a Gauss matrix. If $R_1$ and $R_2$ are independent Gauss matrices, then $R_1 + R_2$ is a Gauss matrix.*

***Proof*** Since 0 and 1 can be regarded as discrete Gauss distributions with parameter $s$ close enough to 0, then $\begin{pmatrix} R \\ I_n \end{pmatrix}$ is also a Gauss matrix. On the other hand, the sum of two independent random variables with Gauss distribution still has Gauss distribution, so $R_1 + R_2$ is a Gauss matrix. The lemma holds. □

Now we discuss the workflow of the GSW fully homomorphic encryption.

Key: the public key is $\overline{A} \in \mathbb{Z}_q^{n \times \overline{m}}, \overline{m} = n + nl$, each column of $\overline{A}$ is an independent sample of the LWE distribution $A_{s,\chi}$ under the private key $\overline{s} \in \mathbb{Z}^{n-1}$. Let $s = \begin{pmatrix} -\overline{s} \\ 1 \end{pmatrix} \in \mathbb{Z}_q^n$, if $\chi$ has discrete Gauss distribution, we have (see 4.1.3 in Chap. 4)

$$s'\overline{A} \equiv_\chi 0 \pmod{q}, \tag{6.3.22}$$

with the private key $s = \begin{pmatrix} -\overline{s} \\ 1 \end{pmatrix} \in \mathbb{Z}_q^n$.

Encryption: let $x \in \mathbb{Z}$ be a plaintext, $f(x)$ be an $n \times nl$ dimensional matrix $A$ encrypted for $x$,

$$f(x) = A = xG - \overline{A}R, \tag{6.3.23}$$

i.e. $A$ is the ciphertext, $G$ is the $n \times nl$ gadget matrix, $R \in \mathbb{Z}_q^{n \times nl}$ is a Gauss matrix.

Decryption: based on (6.3.22), decrypt $A$ with the private key $s = \begin{pmatrix} -\overline{s} \\ 1 \end{pmatrix}$,

$$\begin{aligned} s'A &= xs'G - s'\overline{A}R \\ &\equiv_\chi xs'G \pmod{q}. \end{aligned} \tag{6.3.24}$$

Correctness: since $s'A$ is a given ciphertext matrix, and $G$ is the gadget matrix, by (6.2.8),

$$xs'G \equiv_\chi s'A \pmod{q},$$

we can solve the only one solution $xs'$ with high probability, and get $f^{-1}(A) = x$.

**Theorem 6.3.2** *The GSW encryption system is bounded fully homomorphic encryption, where the addition and multiplication of the ciphertexts are defined as if $A_1 = f(x_1)$, $A_2 = f(x_2)$, then $A_1 + A_2$ is the matrix addition, and*

$$A_1 A_2 = A_1 G^{-1}(A_2) \in \mathbb{Z}_q^{n \times nl} \tag{6.3.25}$$

*is the matrix multiplication.*

***Proof*** The conclusion of theorem 2 is actually implied in lemma 3.3. Let $x_1, x_2 \in \mathbb{Z}_q$ be two plaintexts,

$$\begin{cases} A_1 = f(x_1) = x_1 G - \overline{A} R_1, \\ A_2 = f(x_2) = x_2 G - \overline{A} R_2, \end{cases}$$

then

$$A_1 + A_2 = (x_1 + x_2)G - \overline{A}(R_1 + R_2),$$

so we have (with high probability)

$$f^{-1}(A_1 + A_2) = x_1 + x_2 = f^{-1}(A_1) + f^{-1}(A_2).$$

Let

$$R = x_1 R_2 + R_1 G^{-1}(A_2), \tag{6.3.26}$$

according to (6.3.21),

$$A_1 A_2 = A_1 G^{-1}(A_2) = x_1 x_2 G - \overline{A} R,$$

therefore,

$$f^{-1}(A_1 A_2) = x_1 x_2 = f^{-1}(A_1) f^{-1}(A_2).$$

Since GSW encryption system is based on Gauss distribution, the Gauss matrix in (6.3.23) has errors. The error will be larger by adding and multiplying the ciphertext matrix many times. GSW encryption system is bounded fully homomorphic encryption, so it is necessary to control the error when adding and multiplying the ciphertexts in order to ensure high probability. This is because the larger the error of Gauss distribution, the smaller the probability, and the probability that the above equation holds also decreases. □

To complete the proof of Theorem 6.3.2, we need the following lemma.

**Lemma 6.3.5** *If $R_1$ and $R_2$ are Gauss matrices, then the matrix defined by (6.3.26) is also a Gauss matrix.*

***Proof*** Since both $R_1$ and $R_2$ are Gauss matrices, then $x_1 R_2$ and $R_1 G^{-1}(A_2)$ are Gauss matrices, based on lemma 3.4,

$$R = x_1 R_2 + R_1 G^{-1}(A_2)$$

is a Gauss matrix. Lemma 3.5 holds. □

Finally, we emphasize that the advantage of GSW fully homomorphic encryption is that the dimension of ciphertext multiplication does not increase. The ciphertext multiplication defined by (6.3.25), in fact, $A_1 A_2$ and $A_1$, $A_2$ are in the same ciphertext space.

## 6.4 Construction of Gentry

In 2009, C. Gentry first proposed a bounded algorithm for fully homomorphic encryption, which partially answered the RAD problem. The work by Gentry is an abstract description of fully homomorphic encryption (Garg et al., 2013a, 2013b; Gentry, 2009a, 2009b, 2010; Gentry et al., 2012a, 2012b, 2013a, 2015; Gentry & Halevi, 2011). It is difficult to understand the ideas and technologies by Gentry since there are many linguistic concepts. On the basis of BV fully homomorphic encryption and GSW fully homomorphic encryption in the previous section, it is possible for us to better understand Gentry's ideas and methods.

Recall the working principle of the most representative public key cryptography RSA. Suppose $N$ is the product of two different prime numbers, $pk$ denotes the public key, and the public key of RSA is $pk = (N, e)$, where $1 \leqslant e < \varphi(N)$, $(e, \varphi(N)) = 1$, $\varphi(N)$ is the Euler function of $N$. For any plaintext $\pi_i \in \mathbb{Z}_N$ $(0 \leqslant \pi_i < N)$, the encryption algorithm of RSA is $\psi_i \equiv \pi_i^e \pmod N$, we write

$$\{\psi_i \leftarrow \pi_i^e \bmod N\} \tag{6.4.1}$$

as the cryptosystem of the ciphertext $\psi_i$ encrypted by the plaintext $\pi_i$ using the public key $pk$. If there are $t$ ciphertexts $\{\psi_1, \psi_2, \ldots, \psi_t\}$, obviously,

$$\prod_{i=1}^{t} \psi_i \equiv \left(\prod_{i=1}^{t} \pi_i\right)^e \pmod N,$$

so we have

$$\left\{\prod_{i=1}^{t} \psi_i \leftarrow \left(\prod_{i=1}^{t} \pi_i\right)^e \bmod N\right\},$$

this shows that the product $\prod \psi_i$ of $t$ ciphertexts $\psi_i$ is encrypted by the product $\prod_{i=1}^{t} \pi_i$ of the corresponding $t$ plaintexts $\pi_i$. In other words, the plaintext corresponding to the product of the $t$ ciphertexts is the product of the $t$ plaintexts $\pi_i$. In section 6.1, we use the decryption algorithm to describe this multiplicative homomorphism as

$$f^{-1}\left(\prod_{i=1}^{t} \psi_i\right) = \prod_{i=1}^{t} f^{-1}(\psi_i).$$

In order to define homomorphic encryption more generally, we first introduce the concept of circuit, which is widely used in the computer field.

**Definition 6.4.1** A circuit $C$ on the set $A$ is a multivariate mapping defined on $A$. For any $t$ elements $a_1, a_2, \ldots, a_t \in A$, $C(a_1, a_2, \ldots, a_t)$ is the image of the mapping $C$. From the perspective of computer work, we can take $(a_1, a_2, \ldots, a_t)$ as an input, and $C(a_1, a_2, \ldots, a_t)$ is regarded as one output. Multiple input and output can be viewed as a circuit. If there are multiple circuits $C$ on $A$, the set of these circuits is written as $C_A$.

In a public key cryptosystem $E$, we use $pk$ and $sk$ to represent the public key and the private key respectively. Of course, $pk$ and $sk$ are not just one element, there may be many public and private keys.

**Definition 6.4.2** A public key cryptosystem $E$ with the circuit set $C_E$ is called a fully homomorphic encryption system, if $E$ contains the following four algorithms:

1. Key generated algorithm, denoted as $KG_E$.
2. Encryption algorithm, denoted as $E_{nE}$.
3. Decryption algorithm, denoted as $D_{nE}$.
4. Ciphertext algorithm, denoted as $Eval_E$.

For any public key $pk$, and any circuit $C \in C_E$ on the plaintext space, any $t$ ciphertexts $\psi_1, \psi_2, \ldots, \psi_t$, where

$$\psi_i \leftarrow E_{nE}(pk, \pi_i),\ 1 \leqslant i \leqslant t, \tag{6.4.2}$$

the ciphertext algorithm $Eval_E$ is to compute

$$\psi \leftarrow Eval_E(pk, C, \psi_1, \psi_2, \ldots, \psi_t),$$

where $\psi$ is the encryption of $C(\pi_1, \pi_2, \ldots, \pi_t)$ under the public key $pk$, i.e.

$$\psi \leftarrow E_{nE}(pk, C(\pi_1, \pi_2, \ldots, \pi_t)). \tag{6.4.3}$$

***Remark 6.4.1*** The number of elements of a circuit is denoted as $|C|$, which is called the boundary of the circuit. Usually the computational complexities of $KG_E$, $E_{nE}$, $D_{nE}$ and $Eval_E$ are polynomial of the security parameter $\lambda$ and the circuit boundary $|C|$.

***Remark 6.4.2*** An equivalent form of (6.4.3) is

$$C(\pi_1, \pi_2, \ldots, \pi_t) = D_{nE}(\psi), \tag{6.4.4}$$

that is, the plaintext corresponding to the calculation result $\psi$ under the ciphertext algorithm $Eval_E$ by the $t$ ciphertexts $\psi_1, \psi_2, \ldots, \psi_t$ is the output in the circuit $C(\pi_1, \pi_2, \ldots, \pi_t)$ by $\pi_1, \pi_2, \ldots, \pi_t$. Therefore, in a fully homomorphic encryption system, the plaintext circuit $C$ actually defines the ciphertext circuit $D$, where

$$D(\psi_1, \psi_2, \ldots, \psi_t) = Eval_E(pk, C, \psi_1, \psi_2, \ldots, \psi_t)$$

satisfying

$$D_{nE}(D(\psi_1, \psi_2, \ldots, \psi_t)) = C(\pi_1, \pi_2, \ldots, \pi_t). \tag{6.4.5}$$

The basic idea of Gentry is to construct fully homomorphic encryption on a general ring. In order to prove the security, the ideal of a quotient ring on the rounding function ring $\mathbb{Z}[x]$ is corresponding to an ideal lattice in $\mathbb{Z}^n$ (see Chap. 5), so the construction of Gentry is called fully homomorphic encryption based on ideal lattice now.

Let $R$ be a commutative ring with identity, $I$ and $J$ are two coprime nonzero ideals in $R$, i.e. $I + J = R$, $R/I$ and $R/J$ denote the quotient rings. The construction of Gentry can be divided into the following steps:

① Fix an ideal $I$ of $R$ and a basis $B_I$ of $I$.
② For any ideal $J$ of $R$, $(I, J) = 1$, we give an ideal generating algorithm $\text{IdealGen}(R, B_I)$ to generate the public key basis $B_J^{pk}$ and the private key basis $B_J^{sk}$. In fact, $B_J^{sk}$ could be chosen as another ideal $J_1$ of $R$, such that $J = J_1$, $B_J^{sk} = B_{J_1}$ is the basis of $J_1$.
③ Construct a sampling algorithm $\text{Samp}(x, B_I, R, B_J)$,

$$\text{Samp}(x, B_I, R, B_J) = \text{a representative element of additive coset } x + I = \overline{x}.$$

④ In the ciphertext algorithm any circuit of $R$ is computed in $R/I$, i.e. if $x_1, x_2 \in R/I$, then $C(x_1, x_2) \equiv x_3 \pmod{I}$. Take the addition circuit and the multiplication circuit as an example, for any $x_1, x_2 \in R/I$, $x_1 + x_2 \equiv x_3 \pmod{I}$, there exists only one $x_3$ under the sampling algorithm $\text{Samp}(x, B_I, R, B_J)$, which is denoted as $Add_{B_I}$. Similarly, the multiplication in $R/I$ is denoted as $Mult_{B_I}$.
⑤ Ciphertext generation. Fix a ring $R$ and an ideal $I$ of $R$, then

$$KG(R, B_I) = (B_J^{sk}, B_J^{pk}) \leftarrow \text{IdealGen}(R, B_I),$$

the plaintext space is a representative element set of the quotient ring $R/I$.

The public key contains $R$, $B_I$, $B_J^{pk}$ and the sampling algorithm.
The private key $sk$ contains $B_J^{sk}$.

The encryption algorithm: the plaintext space is $R/I$, for any plaintext $u \in R/I$, based on the sampling algorithm we have $\text{Samp}(u, B_I, R, B_J^{pk}) \to \psi'$, the encryption algorithm $En(pk, u)$ is defined as

$$En(pk, u) = \psi = \psi' \bmod B_J^{pk}.$$

The decryption algorithm $De(sk, \psi)$ is defined as

$$u \leftarrow (\psi \bmod B_J^{sk}) \bmod B_I.$$

The ciphertext algorithm: if $\psi_1$, $\psi_2$ are two ciphertexts, then the addition and multiplication are defined as

$$Add(pk, \psi_1, \psi_2) = \psi_1 + \psi_2 = (\psi_1 + \psi_2) \bmod B_J^{pk},$$

$$Mult(pk, \psi_1, \psi_2) = \psi_1 \psi_2 = (\psi_1 \psi_2) \bmod B_J^{pk}.$$

The key of Gentry's construction is to verify the correctness of encryption and decryption and the homomorphism property of the ciphertext algorithm. We call the above public key generation algorithm, encryption algorithm, decryption algorithm and ciphertext algorithm as the fully homomorphic encryption system of Gentry, denoted as $E$. In order to prove the fully homomorphic property of $E$, we observe that there are two kinds of circuits in $E$. First, the circuit $C$ used for encryption is defined by the addition and multiplication in the quotient ring $R/I$. The other circuit used in the ciphertext algorithm is defined by the addition and multiplication in $R$ itself, which is called the generating circuit.

**Definition 6.4.3** Given a circuit $C$ in the plaintext space, we call $g(C)$ its generating circuit if the operation of mod $B_I$ in $C$ is replaced by the original addition and multiplication.

**Definition 6.4.4** Let $X_{enc}$ be the image of $R/I$ under the sampling algorithm Samp, i.e. $X_{enc}$ is a set of representative elements of $R/I$, and $X_{enc}$ is a plaintext space, so the ciphertext space is $\{X_{enc} + J\}$. Define $X_{Dec}$ as $R$ mod $B_J^{sk}$, i.e. the representation of the elements in $R/J$ under mod $B_J^{sk}$.

**Definition 6.4.5** The circuit satisfying the following condition in the circuit set $C_E$ is called an allowable circuit set,

$$C'_E = \{C : \forall (x_1, x_2, \ldots, x_t) \in X_{enc}^T \Rightarrow g(C)(x_1, x_2, \ldots, x_t) \in X_{Dec}\}. \quad (6.4.6)$$

On the basis of the above definitions and notations, the main conclusion of Gentry is that for any ciphertext [see (6.4.3)] in any allowable circuit, it has the fully homomorphic property.

**Theorem 6.4.1** *Let $C_E$ be an allowable circuit set, then the ciphertext encrypted by any allowable circuit $C$ in $C_E$ has the fully homomorphic property.*

***Proof*** Let $C \in C_E, \psi = \{\psi_1, \psi_2, \ldots, \psi_t\}$, where each $\psi_i$ is the encrypted ciphertext of the allowable circuit, so each ciphertext $\psi_k$ could be written as

$$\psi_k = \pi_k + i_k + j_k,\ \pi_k \in R/I,\ i_k \in I,\ j_k \in J,$$

and $\pi_k + i_k \in X_{enc}$. We have

$$Eval(pk, C, \psi) = g(C)(\psi) \bmod B_J^{pk}$$

$$\in g(C)(\pi_1 + i_1, \pi_2 + i_2, \ldots, \pi_t + i_t) + J.$$

If $C \in C_E$, then

$$g(C)(X_{enc}, X_{enc}, \ldots, X_{enc}) \in X_{Dec},$$

therefore,

$$\begin{aligned} &\text{Decrypt}(sk, Eval(pk, C, \psi)) \\ &= g(C)(\pi_1 + i_1, \pi_2 + i_2, \ldots, \pi_t + i_t) \bmod B_I \\ &= g(C)(\pi_1 + \pi_2 + \cdots + \pi_t) \bmod B_I \\ &= C(\pi_1, \pi_2, \ldots, \pi_t). \end{aligned}$$

Applying the above conclusion to the addition circuit and the multiplication circuit respectively, we get the fully homomorphic property in the allowable circuit. □

We choose $R = \mathbb{Z}[x] / <f(x)>$, where $f(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree $n$. Each polynomial in the quotient ring $R$ corresponds to a vector in $\mathbb{Z}^n$:

$$\alpha(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in R \longleftrightarrow \alpha = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \in \mathbb{Z}^n.$$

Furthermore, the correspondence between the ideal in $R$ and the ideal lattice in $\mathbb{Z}^n$ is one-to-one (see Chap. 5). For example, $I = <\alpha(x)>$ is the principal ideal generated by $\alpha(x) \in R$, then

$$<\alpha(x)> = I \longleftrightarrow L(H^*(\alpha)),$$

where $H^*(\alpha)$ is the ideal matrix generated by $\alpha$, $L(H^*(\alpha))$ is the integral lattice generated by $H^*(\alpha)$. For $I \subset R$, $I$ is not a principal ideal, based on Chap. 5 we know

$$L(I) = \{\alpha \mid \alpha(x) \in I\} \subset \mathbb{Z}^n$$

is an integral lattice. Denote $B_I$ as the generating matrix of $L(I)$, then $B_I$ is the basis of ideal $I$ in the construction of Gentry. In the key generation algorithm constructed by Gentry, the public key is $B_J^{pk}$. We select an ideal $J \subset R$ such that $(I, J) = 1$ with the basis $B_J$, i.e. $J$ is the generating matrix of the corresponding ideal lattice $L(J)$. For convenience,

$$B_J^{pk} = \text{the HNF basis of } L(J)$$

is the Hermite normal basis of $L(J)$. The private key is $B_J^{sk}$, we choose an ideal $J_1$ larger than $J$, i.e. $J \subset J_1 \subset R$, $J_1 \neq J$, so

$$B_J^{sk} = \text{the generating matrix of the ideal lattice } L(J_1).$$

Since $J \subset J_1$, by the homomorphism theorem of ring we have

$$J_1/J \cong (R/J)/(R/J_1).$$

Here $R/J_1$ is a subring of $R/J$, so in the sampling algorithm, for any $a \in R/J$, we can find only one $a_{J_1} \in R/J_1$.

Above all, we can take $R$ as a specific quotient ring $\mathbb{Z}[x] / < f(x) >$ of the integer coefficient polynomial ring $\mathbb{Z}[x]$ to realize the construction of fully homomorphic encryption by Gentry. Since the correspondence between the ideal in $R$ and the ideal lattice in $\mathbb{Z}^n$ is one-to-one, Gentry's construction is widely known as a fully homomorphic encryption system based on the ideal lattice. Because the conclusion is only valid on the set of allowable circuit, it is only a bounded fully homomorphic encryption.

## 6.5 Attribute-Based Encryption

Fully homomorphic digital signature is a research hotspot at present, among which attribute-based encryption is a relatively mature topic. Attribute-based encryption (ABE) is a generalized form of identity-based encryption which is proposed in Goyal et al. (2006) and Sahai and Waters (2005) first. In this section we will briefly introduce ABE.

**Lemma 6.5.1** *Let $q$ be a prime number, $F_q$ be a finite field with $q$ elements, $F_{q^n}$ be an extension of degree $n$ of $F_q$, then $F_{q^n}$ is isomorphic to a subring $\mathcal{H}$ of $\mathbb{Z}_q^{n\times n}$, where $a, b \in \mathcal{H} \Rightarrow a - b \in GL_n(F_q)$, i.e. $a - b$ is an invertible matrix.*

***Proof*** $F_{q^n}$ / $F_q$ is an $n$ dimensional linear space, let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subset F_{q^n}$ be a basis. For any $\alpha \in F_{q^n}$, we define a linear transformation $\tau_\alpha$ on $F_{q^n}$

$$\tau_\alpha(x) = \alpha x, \ x \in F_{q^n}. \tag{6.5.1}$$

Obviously $\tau_\alpha$ is a linear transformation on $F_{q^n}$. Under the given basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, let $A_\alpha$ be the corresponding matrix of $\tau_\alpha$, that is,

$$\tau_\alpha(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_n) = (\alpha_1, \alpha_2, \ldots, \alpha_n)A_\alpha.$$

Let

$$\mathcal{H} = \{A_\alpha \mid \alpha \in F_{q^n}\} \subset \mathbb{Z}_q^{n\times n},$$

we have

$$A_{\alpha+\beta} = A_\alpha + A_\beta,\ A_{\alpha\cdot\beta} = A_\alpha \cdot A_\beta,$$

so $F_{q^n} \to \mathcal{H}$ is a ring isomorphism. Note that if $\alpha \neq 0$, then $\tau_\alpha$ is an invertible linear transformation on $F_{q^n}$, and the corresponding matrix $A_\alpha$ of $\tau_\alpha$ is an invertible matrix. If $a, b \in F_{q^n}, a \neq b$, it follows that $A_{a-b} \in GL_n(F_q)$, in other words, the difference of any two different matrices in the matrix ring $\mathcal{H}$ is an invertible matrix. □

***Remark 6.5.1*** The trace function and determinant of the matrix $A_\alpha$ corresponding to the linear transformation $\tau_\alpha$ are called the trace and norm of $\alpha$, i.e.

$$\mathrm{tr}(\alpha) = \mathrm{tr}(A_\alpha),\ N(\alpha) = \det(A_\alpha),$$

where $\mathrm{tr}(\alpha)$ is an additive homomorphism of $F_{q^n} \to F_q$, and $N(\alpha)$ is a multiplicative Homomorphism of $F_{q^n} \to F_q$.

Let $F_{q^n}$ be an $n$ dimensional linear space of $F_q$. Given a basis, $F_{q^n}$ and $F_q^n$ are isomorphic as the linear spaces of $F_q$. For any elements $\alpha_1, \alpha_2, \ldots, \alpha_l \in F_{q^n}$ in $F_{q^n}$, we can define the inner product based on Lemma 6.5.1.

**Definition 6.5.1** For any $\alpha, \beta \in F_{q^n}$, let $\alpha \to H\alpha \in \mathcal{H}$, $\beta \to H_\beta \in \mathcal{H}$, we define the inner product of $\alpha$ and $\beta$ by

$$<\alpha, \beta> = H_\alpha \cdot H_\beta. \tag{6.5.2}$$

***Remark 6.5.2*** Since $H_\alpha \cdot H_\beta \in F_q^{n\times n}$ is a square matrix of order $n$, the inner product of two field elements is a vector. If $H_\alpha \cdot H_\beta \in \mathcal{H}$, based on lemma 5.1, there exists $\gamma \in F_{q^n} \Rightarrow r \to H_\alpha \cdot H_\beta$. However, we cannot get $\gamma = \alpha \cdot \beta$, which means that (6.5.2) and the one-to-one correspondence of lemma 5.1 are not commutative.

ABE encryption technique is a very complex matrix encryption method. The basic principle is to use the gadget matrix to generate encryption and decryption algorithms based on the LWE distribution. It involves the encryption public key of LWE cryptosystem, and a private key system based on the attribute vector and the dependent vector, which are the keys in the digital signature. In order to fully understand the workflow of ABE, we start with some basic matrices.

Let $q$ be a prime number, $\mathbb{Z}_q$ is equivalent to a finite field with $q$ elements, and $\mathbb{Z}_q^n$ is equivalent to an extension of degree $n$ of $\mathbb{Z}_q$. Let $G$ be a gadget matrix of order $n$ [see (6.2.6)], i.e.

$$G = I_n \otimes g' = \mathrm{diag}\{g', g', \ldots, g'\} \in \mathbb{Z}_q^{n\times nl},$$

where $l = \lfloor \log_2 q \rceil$, define $\overline{A}$ and $A$ by

$$\begin{cases} \overline{A} \in \mathbb{Z}_q^{n\times\overline{m}} \text{ is a uniformly random matrix,} \\ A = [A_1, A_2, \ldots, A_l] \in \mathbb{Z}_q^{n\times wl}, \\ \overline{m} = n + nl, \quad w = nl, \end{cases} \tag{6.5.3}$$

where each $A_i \in \mathbb{Z}_q^{n\times nl}$ has the same dimension with the gadget matrix $G$. Let $\overline{A}$ be the private key, $R \in \mathbb{Z}_q^{\overline{m}\times nl}$ be the trapdoor matrix of $\overline{A}$ with tag $H$, i.e.

$$\overline{A}R \equiv HG \pmod{q}.$$

Based on Lemma 6.5.1, we define the attribute vector $\overrightarrow{n}$ by

$$\overrightarrow{n} = [H_1, H_2, \ldots, H_l] \in \mathcal{H}^l, \tag{6.5.4}$$

where each $H_i \in \mathbb{Z}_q^{n\times n}$ is an invertible matrix, so $\overrightarrow{n} \in \mathbb{Z}_q^{n\times nl}$, let

$$\begin{cases} G_{\overrightarrow{n}} = [H_1G, H_2G, \ldots, H_lG] \in \mathbb{Z}_q^{n\times wl}, \\ A_{\overrightarrow{n}} = A + G_{\overrightarrow{n}} \in \mathbb{Z}_q^{n\times wl}, \end{cases} \tag{6.5.5}$$

the dependent vector $\overrightarrow{p} \in \mathcal{H}^l$ defined by the attribute vector $\overrightarrow{n}$ satisfies

$$<\overrightarrow{n}, \overrightarrow{p}> = 0 \Leftrightarrow \sum_{i=1}^{l} H_iP_i = 0,$$

where $\overrightarrow{p} = [P_1, P_2, \ldots, P_l] \in \mathbb{Z}_q^{n\times nl}$, and each $P_i \in \mathbb{Z}_q^{n\times n}$.

In order to discuss the generated private key by the dependent vector $\overrightarrow{p}$, let $S_{\overrightarrow{p}}$ be

$$S_{\overrightarrow{p}} = \begin{pmatrix} G^{-1}(P_1G) \\ G^{-1}(P_2G) \\ \vdots \\ G^{-1}(P_lG) \end{pmatrix}, \tag{6.5.6}$$

here $G^{-1}(P_iG)$ is an integer matrix given by Definition 2.2.

**Lemma 6.5.2** *Under the above notations, we have*

$$G_{\overrightarrow{n}} \cdot S_{\overrightarrow{p}} = <\overrightarrow{n}, \overrightarrow{p}>G = 0.$$

***Proof*** Combining (6.5.5), (6.5.6) and (6.2.7), it follows that

$$G_{\overrightarrow{n}} \cdot S_{\overrightarrow{p}} = [H_1G, H_2G, \ldots, H_lG] \begin{pmatrix} G^{-1}(P_1G) \\ \vdots \\ G^{-1}(P_lG) \end{pmatrix}$$

$$= H_1GG^{-1}(P_1G) + \cdots + H_lGG^{-1}(P_lG)$$

$$= H_1P_1G + H_2P_2G + \cdots + H_lP_lG$$

$$= (H_1P_1 + H_2P_2 + \cdots + H_lP_l)G$$

$$= <\overrightarrow{n}, \overrightarrow{p}>G = 0.$$

□

Encryption: based on the above definitions, let $u \in \mathbb{Z}_q^n$, we encrypt a single bit $u \in \mathbb{Z}_2$ by the LWE cryptosystem, and the ciphertext $\{\overline{c}, c_{\overrightarrow{n}}, c\}$ satisfies

$$\begin{cases} \overline{c} \equiv_\chi s' \cdot \overline{A} \pmod q, \\ c_{\overrightarrow{n}} \equiv_\chi s' \cdot A_{\overrightarrow{n}} \pmod q, \\ c \equiv_\chi s' \cdot u + u \left\lfloor \frac{q}{2} \right\rceil, \end{cases} \tag{6.5.7}$$

where $s$ is the private key of the LWE cryptosystem.

We write $\{\overline{c}, c_{\overrightarrow{n}}, c\}$ as the following form

$$[\overline{c}', c'_{\overrightarrow{n}}, c] \equiv_\chi s'[\overline{A}, A_{\overrightarrow{n}}, u] + \begin{pmatrix} 0 \\ u \left\lfloor \frac{q}{2} \right\rceil \end{pmatrix} \pmod q.$$

Decryption: generate the private key vector $x_{\overrightarrow{p}}$ satisfying the following equalities by the dependent vector $\overrightarrow{p}$,

$$\begin{cases} [\overline{A}, B_{\overrightarrow{p}}]x_{\overrightarrow{p}} = u, \\ B_{\overrightarrow{p}} = A \cdot S_{\overrightarrow{p}}, \end{cases} \tag{6.5.8}$$

use $x_{\overrightarrow{p}}$ as the private key to decrypt the ciphertext $\{\overline{c}, c_{\overrightarrow{n}}, c\}$ as follows

$$[\overline{c}', c'_{\overrightarrow{n}} \cdot S_{\overrightarrow{p}}] \cdot x_{\overrightarrow{p}},$$

by (6.5.7), we replace the congruence with equality, then (based on Lemma 5.2)

$$c'_{\overrightarrow{n}} \cdot S_{\overrightarrow{p}} = s'A_{\overrightarrow{n}} \cdot S_{\overrightarrow{p}} = s'(A + G_{\overrightarrow{n}})S_{\overrightarrow{p}}$$

$$= s'B_{\overrightarrow{p}} + s'G_{\overrightarrow{n}} \cdot S_{\overrightarrow{p}} = s'B_{\overrightarrow{p}},$$

therefore,

$$[\overline{c}', c'_{\overrightarrow{n}} \cdot S_{\overrightarrow{p}}] \cdot x_{\overrightarrow{p}} \equiv_\chi s'[A', B_{\overrightarrow{p}}] \cdot x_{\overrightarrow{p}} \pmod q$$

$$\equiv_\chi s'u \pmod q$$

$$\equiv c - u \left\lfloor \frac{q}{2} \right\rceil \pmod q$$

$$= u.$$

Both $x_{\overrightarrow{p}}$ and $S_{\overrightarrow{p}}$ are the shortest integer solutions.

We will not verify the fully homomorphic property of ABE here, and leave it to the readers as an exercise. Constructing fully homomorphic digital signature by the ABE encryption technology is a popular research topic at present, and we suggest readers to follow up it further.



# Chapter 7
# A Generalization of NTRUencrypt


NTRU cryptosystem is a new public key cryptosystem based on lattice hard problem proposed in 1996 by three digit theorists Hoffstein, Piper and Silverman of Brown University in the United States. The essence of NTRU cryptographic design is the generalization of RSA on polynomials, so it is called the cryptosystem based on polynomial rings. Its main feature is that the key generation is very simple, and the encryption and decryption algorithm is much faster than the commonly used RSA and elliptic curve cryptography. In particular, NTRU can resist quantum computing attacks and is considered to be a potential public key cryptography that can replace RSA in the post-quantum cryptography era.

Many researchers have presented some variations of NTRU by changing its algebraic structure. In 2002, Gaborit introduced an NTRU-like cryptosystem called CTRU by replacing the base ring of the NTRU with a polynomial ring over a binary field $F_2[x]$ (Gaborit et al., 2002). They proved that their system is successfully decrypted. In 2005, Kouzmenko showed that CTRU is weak under a time attack and proposed the GNTRU cryptosystem based on Gaussian integers (Kouzmenko 2006). In the same year, Coglianese introduced an analog to the NTRU cryptosystem called MaTRU (Coglianese & Goi, 2005). MaTRU is based on a ring of all square matrices with polynomial entries. In 2009, Malekian introduced the QTRU cryptosystem based on quaternion algebra (Malecian et al., 2011). They also introduced the OTRU cryptosystem in 2010 based on Octonion algebra (Malecian & Zakerolhsooeini, 2010). In 2016, Alsaidi proposed a public key cryptosystem BITRU based on binary algebra (Alsaidi & Yassein, 2016). However, all of the above variations of NTRU have limitations. The purpose of this chapter is extending the theory of circulant matrix to general ideal matrix, and constructing more general NTRU cryptosystem combining with the $\phi$-cyclic code. The motivation of this research is to adapt the distributed scenario of blockchain architecture and apply the post-quantum cryptography in it.



Z. Zheng et al., *Modern Cryptography Volume 2*, Financial Mathematics and Fintech,
https://doi.org/10.1007/978-981-19-7644-5_7

## 7.1 $\phi$-Cyclic Code

Let $F_q$ be a finite field with $q$ elements and $q$ be a power of a prime number, $F_q[x]$ be the polynomial ring of $F_q$ with variable $x$. Let $F_q^n$ be the $n$ dimensional linear space over $F_q$, and $\phi = (\phi_0, \phi_1, \ldots, \phi_{n-1}) \in F_q^n$ be a fixed vector in $F_q^n$ with $\phi_0 \neq 0$, the associated polynomial of $\phi$ given by

$$\phi(x) = x^n - \phi_{n-1}x^{n-1} - \cdots - \phi_1 x - \phi_0 \in F_q[x],\ \phi_0 \neq 0. \tag{7.1.1}$$

Let $<\phi(x)>$ be the principal ideal generated by $\phi(x)$ in $F_q[x]$. There is a one-to-one correspondence between $F_q^n$ and the quotient ring $R = F_q[x]\,/\,<\phi(x)>$, given by

$$c = (c_0, c_1, \ldots, c_{n-1}) \in F_q^n \rightleftarrows c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in R. \tag{7.1.2}$$

In fact, this correspondence is also an isomorphism of Abel groups. One may extend this correspondence to subsets of $F_q^n$ and $R$ by

$$C \subset F_q^n \rightleftarrows C(x) = \{c(x) | c \in C\} \subset R. \tag{7.1.3}$$

If $C \subset F_q^n$ is a linear subspace of $F_q^n$ of dimension $k$, then $C$ is called a linear code in coding theory and written by $C = [n, k]$ as usual. Each vector $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ is called a codeword of length $n$. Obviously, $C = [n, 0]$ and $C = [n, n]$ are two trivial codes. Another one is called constant codes, of which is almost trivial given by

$$C = \{(b, b, \ldots, b) | b \in F_q\},\ \text{and}\ C = [n, 1].$$

According to the given polynomial $\phi(x)$ in (7.1.1), we may define a linear transformation $\tau_\phi$ in $F_q^n$,

$$\tau_\phi(c) = \tau_\phi((c_0, c_1, \ldots, c_{n-1})) = (\phi_0 c_{n-1}, c_0 + \phi_1 c_{n-1}, c_1 + \phi_2 c_{n-1}, \ldots, c_{n-2} + \phi_{n-1}c_{n-1}). \tag{7.1.4}$$

It is easily seen that $\tau_\phi : F_q^n \to F_q^n$ is a linear transformation.

**Definition 7.1.1** Let $C \subset F_q^n$ be a linear code. It is called a $\phi$-cyclic code, if

$$\forall c \in C \Rightarrow \tau_\phi(c) \in C. \tag{7.1.5}$$

In other words, a linear code $C$ is a $\phi$-cyclic code, if and only if $C$ is closed under linear transformation $\tau_\phi$. Clearly, if $\phi = (1, 0, \ldots, 0)$, and $\phi(x) = x^n - 1$, then the $\phi$-cyclic code is precisely the ordinary cyclic code (Lopez-Permouth et al., 2009).

***Remark 7.1.1*** The $\phi$-cyclic code we give here is polycyclic code in fact, which firstly appeared in Lopez-Permouth et al. (2009), but we mainly concern for its application

to McEliece and Niederriter's cryptosystems. We first show that there is a one-to-one correspondence between $\phi$-cyclic codes in $F_q^n$ and ideals in $R = F_q[x] / <\phi(x)>$.

**Lemma 7.1.1** *Let $C \subset F_q^n$ be a subset, then $C$ is a $\phi$-cyclic code, if and only if $C(x)$ is an ideal of $R$.*

***Proof*** We use column notation for vector in $F_q^n$, then linear transformation $\tau_\phi$ may be written as

$$\tau_\phi \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} \phi_0 c_{n-1} \\ c_0 + \phi_1 c_{n-1} \\ \vdots \\ c_{n-2} + \phi_{n-1} c_{n-1} \end{pmatrix}, \ \forall c = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} \in F_q^n.$$

Let $T_\phi$ be a $n \times n$ square matrix over $F_q$,

$$T_\phi = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & \phi_0 \\ \hline & & & \phi_1 \\ & I_{n-1} & & \vdots \\ & & & \phi_{n-1} \end{array}\right) \in F_q^{n \times n}, \tag{7.1.6}$$

where $I_{n-1}$ is the $(n-1) \times (n-1)$ unit matrix. The matrix expression of $\tau_\phi$ as follows

$$\tau_\phi \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = T_\phi \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} \phi_0 c_{n-1} \\ c_0 + \phi_1 c_{n-1} \\ \vdots \\ c_{n-2} + \phi_{n-1} c_{n-1} \end{pmatrix}. \tag{7.1.7}$$

Suppose $C \subset F_q^n$ and $C(x)$ is an ideal of $R$, it is clear that $C$ is a linear code of $F_q^n$. To prove $C$ is a $\phi$-cyclic code, we note that for any polynomial $c(x) \in C(x)$, then $xc(x) \in C(x)$ if and only if $\tau_\phi(c) \in C$, namely, if $c(x) \in C(x)$, then

$$xc(x) \in C(x) \Leftrightarrow \tau_\phi(c) \in C \Leftrightarrow T_\phi c \in C. \tag{7.1.8}$$

Therefore, if $C(x)$ is an ideal of $R$, then we have immediately that $C$ is a $\phi$-cyclic code of $F_q^n$.

Conversely, if $C \subset F_q^n$ is a $\phi$-cyclic code, then for all $k \geqslant 1$, we have

$$\forall c \in C \Rightarrow T_\phi^k c \in C.$$

It follows that

$$\forall c(x) \in C(x) \Rightarrow x^k c(x) \in C(x), \ 0 \leqslant k \leqslant n-1,$$

which implies $C(x)$ is an ideal of $R$. This is the proof of Lemma 7.1.1. □

By Lemma 7.1.1, to find a $\phi$-cyclic code, it is enough to find an ideal of $R$. There are two trivial ideals $C(x) = 0$ and $C(x) = R$, the corresponding $\phi$-cyclic codes are $C = [n, 0]$ and $C = F_q^n$ , respectively, which are called trivial $\phi$-cyclic code. To find non-trivial $\phi$-cyclic codes, we make use of homomorphic theorems, which is a standard technique in Algebra. Let $\pi$ be the natural homomorphism from $F_q[x]$ to its quotient ring $R = F_q[x] / <\phi(x)>$, $\ker\pi = <\phi(x)>$,

$$<\phi(x)> \subset N \subset F_q[x] \xrightarrow{\pi} R = F_q[x] / <\phi(x)>, \tag{7.1.9}$$

where $N$ is an ideal of $F_q[x]$, of which is containing $\ker\pi = <\phi(x)>$. Since $F_q[x]$ is a principal ideal domain, then $N = <g(x)>$ is a principal ideal generated by a monic polynomial $g(x) \in F_q[x]$. It is easy to see that

$$<\phi(x)> \subset <g(x)> \Leftrightarrow g(x)|\phi(x).$$

It follows that all ideals $N$ satisfying (7.1.9) are given by

$$\{<g(x)> \mid g(x) \in F_q[x] \text{ is monic and } g(x)|\phi(x)\}.$$

We write by $<g(x)> \bmod \phi(x)$, the image of $<g(x)>$ under $\pi$, it is easy to check

$$<g(x)> \bmod \phi(x) = \{h(x)g(x) \mid h(x) \in F_q[x] \text{ and } \deg h(x) + \deg g(x) < n\}, \tag{7.1.10}$$

more precisely, which is a representative elements set of $<g(x)> \bmod \phi(x)$, by homomorphism theorem in ring theory, all ideals of $R$ given by

$$\{<g(x)> \bmod \phi(x) \mid g(x) \in F_q[x] \text{ is monic and } g(x)|\phi(x)\}. \tag{7.1.11}$$

Let $d$ be the number of monic divisors of $\phi(x)$ in $F_q[x]$, we can get the following corollary immediately.

**Lemma 7.1.2** *The number of $\phi$-cyclic code in $F_q^n$ is $d$.*
*To compare the $\phi$-cyclic code and ordinary cyclic code, we see a simple example.*

***Example 7.1*** Constant code $C$ is always a cyclic code for $1 + x + \cdots + x^{n-1} | x^n - 1$, and its generated polynomial is just $1 + x + \cdots + x^{n-1}$. But constant code $C$ in $F_q^n$ is not always a $\phi$-cyclic code, it is a $\phi$-cyclic code if and only if $1 + x + \cdots + x^{n-1} | \phi(x)$, an equivalent condition for $1 + x + \cdots + x^{n-1} | \phi(x)$ is

$$\phi_{n-1} = \phi_{n-2} = \cdots = \phi_1 = b, \text{ and } \phi_0 = 1 + b.$$

**Definition 7.1.2** Let $C$ be a $\phi$-cyclic code and $C(x) = g(x) \bmod \phi(x)$. We call $g(x)$ is the generated polynomial of $C$, where $g(x)$ is monic and $g(x)|\phi(x)$.

**Lemma 7.1.3** *Let $g(x) = g_0 + g_1 x + \cdots + g_{n-k-1}x^{n-k-1} + x^{n-k}$ be the generated polynomial of a $\phi$-cyclic code $C$, where $1 \leqslant k \leqslant n-1$, and $g(x)|\phi(x)$, then $C = [n, k]$ and a generated matrix for $C$ is the following block matrix*

$$G = \begin{pmatrix} g \\ \tau_\phi(g) \\ \tau_\phi^2(g) \\ \vdots \\ \tau_\phi^{k-1}(g) \end{pmatrix}_{k\times n}, \tag{7.1.12}$$

*where $g = (g_0, g_1, \ldots, g_{n-k-1}, 1, 0, \ldots, 0) \in C$ is the corresponding codeword of $g(x)$, and $\tau_\phi^i(g) = \tau_\phi^{i-1}(\tau_\phi(g))$ for $1 \leqslant i \leqslant n-1$.*

***Proof*** By assumption, $C(x) = <g(x)> \bmod \phi(x)$, then $\{g, \tau_\phi(g), \ldots, \tau_\phi^{k-1}(g)\} \subset C$, we are to prove it is a basis of $C$. First, these vectors are linearly independent. Otherwise, we have

$$\sum_{i=0}^{k-1} b_i \tau_\phi^i(g) = 0,\ b_i \in F_q, \tag{7.1.13}$$

and the corresponding polynomial is zero, namely

$$\left(\sum_{i=0}^{k-1} b_i x^i\right) g(x) = 0.$$

It follows that

$$\sum_{i=0}^{k-1} b_i x^i = 0 \Rightarrow b_i = 0 \text{ for all } 0 \leqslant i \leqslant k-1.$$

Next, if $c \in C$, and $c(x) \in C(x)$, by (7.1.10), there is a polynomial $b(x) = b_0 + b_1 x + \cdots + b_{k-2}x^{k-2} + x^{k-1}$ such that

$$c(x) = b(x)g(x) = \left(\sum_{i=0}^{k-1} b_i x^i\right) g(x),\quad b_{k-1} = 1,$$

Thus we have the corresponding codeword of $C(x)$

$$c = \sum_{i=0}^{k-1} b_i \tau_\phi^i(g).$$

This shows that $\{g, \tau_\phi(g), \ldots, \tau_\phi^{k-1}(g)\}$ is a basis of $C$, and a generated matrix for $C$ is

$$G = \begin{pmatrix} g \\ \tau_\phi(g) \\ \tau_\phi^2(g) \\ \vdots \\ \tau_\phi^{k-1}(g) \end{pmatrix}_{k\times n}.$$

We have Lemma 7.1.3 at once. □

To describe a parity check matrix for a $\phi$-cyclic code, for any $c = (c_0, c_1, \ldots, c_{n-1}) \in F_q^n$, we write

$$\overline{c} = (c_{n-1}, c_{n-2}, \ldots, c_1, c_0) \in F_q^n.$$

**Lemma 7.1.4** *Suppose $C$ is a $\phi$-cyclic code with generated polynomial $g(x)$, where $g(x)|\phi(x)$ and $degg(x) = n - k$. Let $h(x)g(x) = \phi(x)$, where $h(x) = h_0 + h_1 x + \cdots + h_{k-1}x^{k-1} + x^k$. Then a parity check matrix for $C$ is*

$$H = \begin{pmatrix} \overline{h} \\ \tau_\phi(\overline{h}) \\ \vdots \\ \tau_\phi^{n-k-1}(\overline{h}) \end{pmatrix}_{(n-k)\times n}. \tag{7.1.14}$$

***Proof*** Since $h(x)g(x) = \phi(x)$, it means that $h(x)g(x) = 0$ in $R = F_q[x]/<\phi(x)>$; thus we have

$$g_0 h_i + g_1 h_{i-1} + \cdots + g_{n-k} h_{i-n+k} = 0, \ \forall 0 \leqslant i \leqslant n-1,$$

It follows that $GH' = 0$, where $G$ is a generated matrix for $C$ given by (7.1.12). Therefore, $H$ is a parity check matrix for $C$. □

A separable polynomial in Algebra means that it has no multiple roots in its splitting field. The following lemma shows that there is an unit element in any non-zero ideal of $R$, when $\phi(x)$ is a separable polynomial.

**Lemma 7.1.5** *Suppose $\phi(x)$ is a separable polynomial of $F_q$, and $C(x) = g(x)$ mod $\phi(x)$ is an ideal of $R$ with $degg(x) \leqslant n-1$, then there exists an element $d(x) \in C(x)$ such that*

$$c(x)d(x) = c(x), \ \forall c(x) \in C(x).$$

***Proof*** Let $h(x)g(x) = \phi(x)$. Since $\phi(x)$ is a separable polynomial, then $\gcd(g(x), h(x)) = 1$, and there are two polynomial $a(x)$ and $b(x)$ in $F_q[x]$ such that

$$a(x)g(x) + b(x)h(x) = 1.$$

Let

$$d(x) = a(x)g(x) = 1 - b(x)h(x) \in C(x).$$

If $c(x) \in C(x)$, by (7.1.10), we write $c(x) = g(x)g_1(x)$, it follows that

$$c(x)d(x) \equiv a(x)g(x)g(x)g_1(x) \equiv (1 - b(x)h(x))g(x)g_1(x)$$

$$\equiv g(x)g_1(x) \equiv c(x)(\text{mod } \phi(x)).$$

Thus we have $c(x)d(x) = c(x)$ in $R$. □

Next, we discuss maximal $\phi$-cyclic code. Let $C(x) = g(x) \bmod \phi(x)$, and $g(x)$ be an irreducible polynomial in $F_q[x]$, we call the corresponding $\phi$-cyclic code $C$ a maximal $\phi$-cyclic code, because $<g(x)>$ is a maximal ideal in $F_q[x]$.

**Lemma 7.1.6** *Let $C$ be a maximal $\phi$-cyclic code with generated polynomial $g(x)$, $\beta$ be a root of $g(x)$ in some extensions of $F_q$, then*

$$C(x) = \{a(x) \mid a(x) \in R \text{ and } a(\beta) = 0\}. \tag{7.1.15}$$

***Proof*** If $a(x) \in C(x)$, by (7.1.10) we have $a(\beta) = 0$ immediately. Conversely, if $a(x) \in F_q[x]$ and $a(\beta) = 0$, since $g(x)$ is irreducible, thus we have $g(x)|a(x)$, and (7.1.15) follows at once. □

An important application of maximal $\phi$-cyclic code is to construct an error-correcting code, so that we may obtain a modified McEliece-Niederriter's cryptosystem. To do this, let $1 \leqslant m < \sqrt{n}$, and $F_{q^m}$ be an extension field of $F_q$ of degree $m$. Suppose $F_{q^m} = F_q(\theta)$, where $\theta$ is a primitive element of $F_{q^m}$ and $F_q(\theta)$ is the simple extension containing $F_q$ and $\theta$. Let $g(x) \in F_q[x]$ be the minimum polynomial of $\theta$, then $g(x)$ is an irreducible polynomial of degree $m$ of $F_q[x]$. It is well known that $F_{q^m}$ is a Galois extension of $F_q$, so that all roots of $g(x)$ are in $F_{q^m}$. Let $\beta_1, \beta_2, \ldots, \beta_m$ be all roots of $g(x)$, the Vandermonde matrix $V(\beta_1, \beta_2, \ldots, \beta_m)$ defined by

$$H = V(\beta_1, \beta_2, \ldots, \beta_m) = \begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta_m & \beta_m^2 & \cdots & \beta_m^{n-1} \end{pmatrix}_{m \times n}, \tag{7.1.16}$$

where $\beta_1 = \theta$ and each $\beta_i$ is a vector of $(F_q)^m$. For arbitrary monic polynomial $h(x) \in F_q[x]$, $\deg h(x) = n - m$, let $\phi(x) = h(x)g(x)$ and $C$ be a maximal $\phi$-cyclic code generated by $g(x)$. It is easy to verify that

$$c \in C \Leftrightarrow cH' = 0.$$

Therefore, $H$ is a parity check matrix for $C$. If we choose the primitive element $\theta$, so that any $d-1$ columns in $H$ are linearly independent, then the minimum distance of $C$ is greater than $d$, and $C$ is a t-error-correcting code, where $t = [\frac{d}{2}]$.

The public key cryptosystems based on algebraic coding theory were created by Lyubashevsky and Micciancio (2006), and Micciancio and Regev (2009) a suitable t-error-correcting code plays a key role in their construction. The error-correcting code $C$ should satisfy the following requirements:

1. $C$ should have a relatively large error-correcting capability so that a reasonable number of message vectors can be used;
2. $C$ should allow an efficient decoding algorithm so that the decryption can be carried out with a short time.

Our results supply a different way to choose an error-correcting code by selecting arbitrary irreducible polynomials $g(x) \in F_q[x]$ of degree $m$ and roots of $g(x)$ rather than an irreducible factor of $x^n - 1$ and the roots of unit.

In fact, for any positive integer $m$, there is at least an irreducible polynomial $g(x) \in F_q[x]$ with degree $m$. Let $N_q(m)$ be the number of irreducible polynomials of degree $m$ in $F_q[x]$, then we have (see Theorem 3.25 of Lidl & Niederreiter, 1983)

$$N_q(m) = \frac{1}{m}\sum_{d|m} u(\frac{m}{d})q^d = \frac{1}{m}\sum_{d|m} u(d)q^{\frac{m}{d}},$$

where $u(d)$ is Mobiüs function.

Assuming one has selected two monic and irreducible polynomials $g(x)$ and $h(x)$ with $\deg g(x) = m$ and $\deg h(x) = n - m$, let $\phi(x) = g(x)h(x)$, then one may obtain $\phi$-cyclic code $C$ generated by $g(x)$ or $h(x)$, which is more convenient and more flexible than the ordinary methods.

It's difficult to compare the error-correcting capability between $\phi$-cyclic code with existing cyclic codes of the same length and dimension. However, we believe that the advantages of $\phi$-cyclic code will become more clear when $q$ increases.

## 7.2 A Generalization of NTRUencrypt

The public key cryptosystem NTRU proposed in 1996 by Hoffstein, Pipher and Silverman is the fastest known lattice-based encryption scheme; although its description relies on arithmetic over polynomial quotient ring $Z[x]/<x^n - 1>$, it was easily observed that it could be expressed as a lattice-based cryptosystem (see IEEE, 2000). For the background materials, we refer to Hoffstein et al. (1998), Lint (1999), McEliece (1978). Our strategy in this section is to replace $Z[x]/<x^n - 1>$ by more general polynomial ring $Z[x]/<\phi(x)>$ and obtain a generalization of NTRUEncrypt, where $\phi(x)$ is a monic polynomial of degree $n$ with integer coefficients.

In this section, we denote $\phi(x)$ and $R$ by

$$\phi(x) = x^n - \phi_{n-1}x^{n-1} - \cdots - \phi_1 x - \phi_0 \in \mathbb{Z}[x],\ R = \mathbb{Z}[x]/<\phi(x)>,\ \phi_0 \neq 0. \tag{7.2.1}$$

Let $H_\phi \in Z^{n\times n}$ be a square matrix given by

$$H = H_\phi = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & \phi_0 \\ \hline & & & \phi_1 \\ & I_{n-1} & & \vdots \\ & & & \phi_{n-1} \end{array}\right)_{n\times n}, \tag{7.2.2}$$

where $I_{n-1}$ is $(n-1)\times(n-1)$ unit matrix. As described in Chap. 5, $\phi(x)$ is the characteristic polynomial of $H$, and $H$ defines a linear transformation of $\mathbb{R}^n \to \mathbb{R}^n$ by $x \to Hx$, where $x$ is a column vector of $\mathbb{R}^n$. We may extend this transformation to $\mathbb{R}^{2n}$ and denote $\sigma$ by

$$\sigma\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}H\alpha\\ H\beta\end{pmatrix},\ \text{where}\ \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \in \mathbb{R}^{2n}. \tag{7.2.3}$$

Of course, $\sigma$ is again a linear transformation of $\mathbb{R}^{2n} \to \mathbb{R}^{2n}$.

A $q$-ary lattice is a lattice $L$ such that $qZ^n \subset L \subset Z^n$, where $q$ is a positive integer. We give the following definition of convolutional modular lattice.

**Definition 7.2.1** A $q$-ary lattice $L$ is called convolutional modular lattice, if $L$ is in even dimension $2n$ satisfying

$$\forall\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \in L \Rightarrow \sigma\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}H\alpha\\ H\beta\end{pmatrix} \in L, \tag{7.2.4}$$

here $\alpha$ and $\beta$ are column vectors in $\mathbb{R}^n$. In other words, a convolutional modular lattice is a $q$-ary lattice in even dimension and is closed under the linear transformation $\sigma$.

Recalling the secret key $\begin{pmatrix}f\\ g\end{pmatrix}$ of NTRU is a pair of polynomials of degree $n-1$, we may regard $f$ and $g$ as column vectors in $Z^n$. To obtain a convolutional modular lattice containing $\begin{pmatrix}f\\ g\end{pmatrix}$, we need some help of ideal matrices. In Chap. 5, we introduce the definition of ideal matrix generated by a vector $f$,

$$H^*(f) = H^*_\phi(f) = [f, Hf, H^2 f, \ldots, H^{n-1}f]_{n\times n}, \tag{7.2.5}$$

which is a block matrix in terms of each column $H^k f$ $(0 \leqslant k \leqslant n-1)$. It is easily seen that $H^*(f)$ is a generalization of the classical circulant matrices. In fact, if

$$\phi(x) = x^n - 1,\ f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} \in \mathbb{Z}[x],$$

the ideal matrix $H^*_\phi(f)$ generated by $f$ is given by

$$H^*(f) = \begin{pmatrix} f_0 & f_{n-1} & \cdots & f_1 \\ f_1 & f_0 & \cdots & f_2 \\ \vdots & \vdots & & \vdots \\ f_{n-1} & f_{n-2} & \cdots & f_0 \end{pmatrix}, \ \phi(x) = x^n - 1,$$

which is known as a circulant matrix. On the other hand, ideal matrix and ideal lattice play an important role in Ajtai's construction of a collision-resistant Hash function, the related materials we refer to Ajtai and Dwork (1997), Ajtai (1996), Lint (1999).

We have given some properties of ideal matrix from Lemmas 5.2.1–5.2.4 in Chap. 5. Based on these lemmas, next we construct a convolutional modular lattice containing vector $\begin{pmatrix} f \\ g \end{pmatrix}$. Let $\begin{pmatrix} f \\ g \end{pmatrix} \in Z^{2n}$, $(H^*(f))^T$ be the transpose of $H^*(f)$, and

$$A = [(H^*(f))^T, (H^*(g))^T] = \begin{pmatrix} f^T & g^T \\ f^T H^T & g^T H^T \\ f^T (H^T)^2 & g^T (H^T)^2 \\ \vdots & \vdots \\ f^T (H^T)^{n-1} & g^T (H^T)^{n-1} \end{pmatrix}_{n \times 2n}, \tag{7.2.6}$$

$$A^T = \begin{pmatrix} H^*(f) \\ H^*(g) \end{pmatrix} = \begin{pmatrix} f & Hf & \cdots & H^{n-1} f \\ g & Hg & \cdots & H^{n-1} g \end{pmatrix}_{2n \times n}. \tag{7.2.7}$$

We consider $A$ and $A^T$ as matrices over $Z_q$, i.e. $A \in Z_q^{n \times 2n}$, $A^T \in Z_q^{2n \times n}$, a $q$-ary lattice $\Lambda_q(A)$ is defined by

$$\Lambda_q(A) = \{y \in \mathbb{Z}^{2n} \mid \text{there exists } x \in \mathbb{Z}^n \Rightarrow y \equiv A^T x \ (\text{mod } q)\}. \tag{7.2.8}$$

Under the above notations, we prove that $\Lambda_q(A)$ is the convolutional modular lattice containing $\begin{pmatrix} f \\ g \end{pmatrix}$.

**Theorem 7.2.1** *For any column vectors $f \in Z^n$ and $g \in Z^n$, $\Lambda_q(A)$ is a convolutional modular lattice, and*

$$\begin{pmatrix} f \\ g \end{pmatrix} \in \Lambda_q(A).$$

***Proof*** It is known that $\Lambda_q(A)$ is a $q$-ary lattice, i.e.

$$q\mathbb{Z}^{2n} \subset \Lambda_q(A) \subset \mathbb{Z}^{2n}.$$

We only prove that $\Lambda_q(A)$ is fixed under the linear transformation $\sigma$ given by (7.2.4). If $y \in \Lambda_q(A)$, then $y \equiv A^T x \ (\text{mod } q)$ for some $x \in Z^n$, by Lemma 5.2.1 in Chap. 5, we have

$$\sigma(y) \equiv \begin{pmatrix} HH^*(f)x \\ HH^*(g)x \end{pmatrix} = \begin{pmatrix} H^*(f)Hx \\ H^*(g)Hx \end{pmatrix} \equiv A^T Hx \pmod{q}.$$

It means that $\sigma(y) \in \Lambda_q(A)$ whenever $y \in \Lambda_q(A)$. Let

$$e = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{Z}^n \Rightarrow H^*(f)e = f, \text{ and } H^*(g)e = g.$$

We have

$$\begin{pmatrix} f \\ g \end{pmatrix} \in \Lambda_q(A).$$

Theorem 7.2.1 follows. □

Since $\Lambda_q(A) \subset Z^{2n}$, then there is a unique Hermite Normal Form of basis $N$, which is a upper triangular matrix given by

$$N = \begin{pmatrix} I_n & H^*(h) \\ 0 & qI_n \end{pmatrix}, \text{ where } h \equiv (H^*(f))^{-1} g \pmod{q}. \tag{7.2.9}$$

Next, we consider parameters system of NTRU. To choose the parameters of NTRU, let $d_f$ be a positive integer and $\{p, 0, -p\}^n \subset Z^n$ be a subset of $Z^n$, of which has exactly $d_f + 1$ positive entries and $d_f$ negative ones, the remaining $n - 2d_f - 1$ entries will be zero. We take some assumption conditions for choice of parameters as follows:

1. $\phi(x) = x^n - \phi_{n-1}x^{n-1} - \cdots - \phi_1 x - \phi_0 \in \mathbb{Z}[x]$ with $\phi_0 \neq 0$, and $\phi(x)$ is separable polynomial, $n$, $p$, $q$, $d_f$ are positive integers with $n$ prime, $1 < p < q$ and $\gcd(p, q) = 1$.
2. $f(x)$ and $g(x)$ are two polynomials in $Z[x]$ of degree $n - 1$, the constant term of $f(x)$ is 1, $f - 1$ and $g$ are the corresponding vector of $f(x) - 1$ and $g(x)$, such that
$$f - 1 \in \{p, 0, -p\}^n, \quad g \in \{p, 0, -p\}^n.$$
3. $H^*(f)$ is invertible modulo $q$.
4. $d_f < (\frac{q}{2} - 1)/4p - \frac{1}{2}$.

Under the above conditions, by Lemma 5.2.2 in Chap. 5 we have

$$H^*(f) \equiv I_n \pmod{p}, \text{ and } H^*(g) \equiv 0 \pmod{p}. \tag{7.2.10}$$

Now, we state a generalization of NTRU as follows.

1. Private key. The private key in generalized NTRU is a short vector $\begin{pmatrix} f \\ g \end{pmatrix} \in Z^{2n}$, and $\Lambda_q(A)$ is the convolutional modular lattice containing private key.
2. Public key. The public key of the generalized NTRU is the HNF basis $N$ of $\Lambda_q(A)$, which is given by (7.2.9).
3. Encryption. An input message is encoded as a vector $m \in \{1, 0, -1\}^n$ with exactly $d_f + 1$ positive entries and $d_f$ negative ones. Here the reason for restricting $d_f + 1$ positive and $d_f$ negative entries of vector $m$ is to improve the efficiency of encryption and decryption and it's not necessary. The vector $m$ is concatenated with a randomly chosen vector $r \in \{1, 0, -1\}^n$ also with exactly $d_f + 1$ positive entries and $d_f$ negative ones, to obtain a short error vector $\begin{pmatrix} m \\ r \end{pmatrix} \in \{1, 0, -1\}^{2n}$. Let
$$\begin{pmatrix} c \\ 0 \end{pmatrix} = N \begin{pmatrix} m \\ r \end{pmatrix} \equiv \begin{pmatrix} m + H^*(h)r \\ 0 \end{pmatrix} \pmod{q}, \tag{7.2.11}$$
where $h$ is given by (7.2.9). Then, the $n$ dimensional vector $c$
$$c \equiv m + H^*(h)r \pmod{q}$$
is the ciphertext.
4. Decryption. Suppose the entries of $n$ dimensional vector $c$ are belong to interval $[-\frac{q}{2}, \frac{q}{2}]$, then ciphertext $c$ is decrypted by multiplying it by the secret matrix $H^*(f) \bmod q$, it follows that
$$H^*(f)c \equiv H^*(f)m + H^*(f)H^*(h)r \equiv H^*(f)m + H^*(g)r \pmod{q}. \tag{7.2.12}$$
Here, we use (ii) of lemma 5.2.4 in Chap. 5, namely,
$$H^*(f)H^*(g) = H^*(H^*(f)g),$$
If the above four conditions are satisfied, it is easily seen that the coordinates of vector $H^*(f)m + H^*(g)r$ are all bounded by $\frac{q}{2}$ in absolute value, or, with high probability, even for larger value of $d_f$. The decryption process is completed by reducing (7.2.12) modulo $p$, to obtain
$$H^*(f)m + H^*(g)r \equiv mI_n \pmod{p}.$$
Thus one gets plaintext $m$ from ciphertext $c$. We finish the procedure of our general NTRU cryptography.

At the end of this section, we give an example to show the correctness of decryption of general NTRU cryptography.

***Example 7.2*** Let $n = 3$, $p = 3$, $q = 7$, $\phi(x) = x^3 + x^2 + x + 1$, $f(x) = 3x^2 + 1$, $g(x) = 3x^2$, i.e. the private key is $\begin{pmatrix} f \\ g \end{pmatrix}$ with

$$f = \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix}, \ g = \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}.$$

It is easy to get

$$H^*(f) = \begin{pmatrix} 1 & -3 & 3 \\ 0 & -2 & 0 \\ 3 & -3 & 1 \end{pmatrix}$$

and

$$H^*(g) = \begin{pmatrix} 0 & -3 & 3 \\ 0 & -3 & 0 \\ 3 & -3 & 0 \end{pmatrix}.$$

By (7.2.9), we compute $h$ and $H^*(h)$ as follows

$$h \equiv (H^*(f))^{-1} g \pmod{q} = \begin{pmatrix} 2 \\ 0 \\ -3 \end{pmatrix},$$

$$H^*(h) = \begin{pmatrix} 2 & 3 & -3 \\ 0 & 5 & 0 \\ -3 & 3 & 2 \end{pmatrix},$$

then the public key $N$ is

$$N = \begin{pmatrix} I_3 & H^*(h) \\ 0 & 7I_3 \end{pmatrix}.$$

Assume the input message and random vector are

$$m = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \ r = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

we get the ciphertext by (7.2.11)

$$c \equiv m + H^*(h) r \equiv \begin{pmatrix} -3 \\ -2 \\ 3 \end{pmatrix} \pmod{7}.$$

From (7.2.12) we have

$$H^*(f) c \equiv \begin{pmatrix} -2 \\ -3 \\ 0 \end{pmatrix} \pmod{7}.$$

Since

$$\begin{pmatrix} -2 \\ -3 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \pmod 3,$$

one can get the plaintext $m$ from ciphertext $c$,

$$m = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

So we verify the correctness and effectiveness of the general NTRU cryptography.



# References


Agrawal, S., Boneh, D., & Boyen, X. (2010). Efficient lattice (H)IBE in the standard model. In *EUROCRYPT* (pp. 553–572).

Ajtai, M. (1999). Generating hard instances of the short basis problem. In *ICALP* (pp. 1–9).

Ajtai, M. (2004). Generating hard instances of lattice problems. *Quaderni di Matematica,13*, 1–32 (Preliminary version in STOC 1996).

Ajtai, M., & Dwork, C. (1997). A public-key cryptosystem with worst-case/average-case equivalence. In *STOC* (pp. 284–293).

Alperin-Sheriff, J., & Peikert, C. (2013). Practical bootstrapping in quasilinear time. In *CRYPTO* (pp. 1–20).

Alsaidi, M., & Yassein, R. (2016). BITRU: Binary version of the NTRU public key cryptosystem via binary algebra. *International Journal of Advanced Computer Science and Applications, 7*, 1–6.

Alwen J., & Peikert, C. (2011). Generating shorter bases for hard random lattices. *Theory of Computing Systems,48*(3), 535–C553 (Preliminary version in STACS 2009).

Babai, L. (1986). On Lovasz' lattice reduction and the nearest lattice point problem. *Combinatorica,6*(1), 1–13 (Preliminary version in STACS 1985).

Banaszczyk, W. (1993). New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen, 296*(4), 625–635.

Blum, A., Kalai, A., & Wasserman, H. (2003). Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of ACM, 50*(4), 506–519.

Brakerski, Z., & Vaikuntanathan, V. (2011a). Fully homomorphic encryption from ring-LWE and security for key dependent messages. In *CRYPTO* (pp. 505–524).

Brakerski, Z., & Vaikuntanathan, V. (2011b). Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal of Computing,43*(2), 831–871 (Preliminary version in FOCS 2011).

Brakerski, Z., & Vaikuntanathan, V. (2014). Lattice-based FHE as secure as PKE. In *ITCS* (pp. 1–12).

Brakerski, Z., & Vaikuntanathan, V. (2015). Constrained key-homomorphic PRFs from standard lattice assumptions—or: How to secretly embed a circuit in your PRF. In *TCC* (pp. 1–30).

Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2014). (Leveled) fully homomorphic encryption without bootstrapping. *TOCT,6*(3), 13 (Preliminary version in ITCS 2012).

Cassels, J. (1863). *Introduction to diophantine approximation*. Cambridge University Press.

Coglianese, M., & Goi, B. (2005). *MaTRU: A new NTRU based cryptosystem* (pp. 232–243). Berlin, Heidelberg: Springer.




Z. Zheng et al., *Modern Cryptography Volume 2*, Financial Mathematics and Fintech,
https://doi.org/10.1007/978-981-19-7644-5

Davis, P. (1994). *Circulant matrices* (2nd ed.). Chelsea Publishing.
Gaborit, P., Ohler, J., & Soli, P. (2002). *CTRU, a polynomial analogue of NTRU* (p. 4621). RR: Hal Inria.
Garg, S., Gentry, C., & Halevi, S. (2013a). Candidate multilinear maps from ideal lattices. In *EUROCRYPT* (pp. 1–17).
Garg, S., Gentry, C., Halevi, S., Raykova, M., Sahai, A., & Waters, B. (2013b). Candidate indistinguishability obfuscation and functional encryption for all circuits. In *FOCS* (pp. 40–49).
Gentry, C. (2009a). Fully homomorphic encryption using ideal lattices. In *STOC* (pp. 169–178).
Gentry, C. (2009b). *A fully homomorphic encryption scheme* (Ph.D. thesis). Stanford University. http://crypto.stanford.edu/craig
Gentry, C., & Halevi, S. (2011). Implementing Gentry's fully-homomorphic encryption scheme. In *EUROCRYPT* (pp. 129–148).
Gentry, C., Gorbunov, S., & Halevi, S. (2015). Graph-induced multilinear maps from lattices. In *TCC* (pp. 498–527).
Gentry, C., Halevi, S., & Smart, N. P. (2012a). Better bootstrapping in fully homomorphic encryption. In *Public key cryptography* (pp. 1–16).
Gentry, C., Halevi, S., & Smart, N. P. (2012b). Fully homomorphic encryption with polylog overhead. In *EUROCRYPT* (pp. 465–482).
Gentry, C., Halevi, S., Peikert, C., & Smart, N. P. (2013a). Field switching in BGV-style homomorphic encryption. *Journal of Computer Security,21*(5), 663–684 (Preliminary version in SCN 2012).
Gentry, C., Sahai, A., & Waters, B. (2013b). Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *CRYPTO* (pp. 75–92).
Gentry, C. (2010). Computing arbitrary functions of encrypted data. *Communications of the ACM, 53*(3), 97–105.
Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In *CCS*, (pp. 89–98).
Hoffstein, J., Pipher, J., & Silverman, J. (1998). *NTRU: A ring based public key cryptosystem*. Lecture Notes in Computer Science (Vol. 1423, pp. 267–288). Springer, Berlin, Heidelberg.
IEEE Computer Society. (2000). IEEE standard specifications for public-key cryptography. *IEEE Standards, 1363–2000*, 1–228.
Impagliazzo, R., & Zuckerman, D. (1989). How to recycle random bits. In *Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science (FOCS)* (pp. 248–253).
Kouzmenko, R. (2006). *Generalizations of the NTRU cryptosystem*. Ecole Polytechnique Federale de Lausanne: Diploma Project.
Lenstra, A. K., Lenstra, H. W., Jr., & Lovasz, L. (1982). Factoring polynomials with rational coefficients. *Mathematische Annalen, 261*(4), 515–534.
Lidl, R., & Niederreiter, H. (1983). Finite fields. *Encyclopedia of Math. and Its Applications,20*
Lint, J. (1999). *Introduction to coding theory*. Springer.
Lopez-Permouth, S., Parra-Avila, B., & Szabo, S. (2009). Dual generalizations of the concept of cyclicity of codes. *Advances in Mathematics of Communications, 3*, 227–234.
Lyubashevsky, V., & Micciancio, D. (2006). Generalized compact knapsacks are collision resistant. *In ICALP* (Vol. 2, pp. 144–155).
Lyubashevsky, V., Peikert, C., & Regev, O. (2013). On ideal lattices and learning with errors over rings. *Journal of the ACM,60*(6), 43:1–43:35 (Preliminary version in Eurocrypt 2010).
Malecian, E., & Zakerolhsooeini, A. (2010). *OTRU: A non-associative and high speed public key cryptosystem* (pp. 83–90). IEEE Computer Society.
Malecian, E., Zakerolhsooeini, A., & Mashatan, A. (2011). QTRU: A lattice attack resistant version of NTRU PCKS based on quaternion algebra. *The ISC International Journal of Information Security, 3*, 29–42.
McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. In *DSN Progress Report* (pp. 42–44). Jet Propulsion Laboratory.

Micciancio, D. (2007). Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Computational Complexity*, *16*(4), 365–411 (Preliminary version in FOCS 2002).
Micciancio, D., & Regev, O. (2007). Worst-case to average-case reductions based on Gaussian measures. *SIAM Journal of Computing,37*(1), 267–302 (Preliminary version in FOCS 2004).
Micciancio, D., & Regev, O. (2009). Lattice-based cryptography. In *Post Quantum Cryptography,* (pp. 147–191). Springer.
Nielsen, M., & Chuang, I. (2000). *Quantum computation and quantum information*. Cambridge University Press.
Peikert, C. (2009). Public-key cryptosystems from the worst-case shortest vector problem. In *STOC* (pp. 333–342).
Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*
Peikert, C., & Waters, B. (2011). Lossy trapdoor functions and their applications. *SIAM Journal of Computing,40*(6), 1803–1844 (Preliminary version in STOC 2008).
Regev, O. (2004). *Lecture notes on lattices in computer science*. Available at http://www.cs.tau.ac.il/~odedr/teaching/lattices_fall_2004/index.html. Last accessed February 28, 2008.
Regev, O. (2004). New lattice-based cryptographic constructions. *Journal of ACM,51*(6), 899–942 (Preliminary version in STOC 2003).
Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of ACM,56*(6), 1–40 (Preliminary version in STOC 2005).
Regev, O. (2010). The learning with errors problem (invited survey). In *IEEE Conference on Computational Complexity* (pp. 191–204).
Riauba, B. (1975). A central limit theorem for dependent random variables. *Lithuanian Mathematical Journal,* 185–200.
Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. *Foundations of Secure Computation, 4*(11), 169–180.
Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In *EUROCRYPT* (pp. 457–473).
Shi, B. (2018). The spectral norms of geometric circulant matrices with the generalized k-Horadam numbers. *Journal of Inequalities and Applications,14*.
Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal Computing, 26*(5), 1484–1509.
Yasin, Y., & Taskara, N. (2013). On the inverse of circulant matrix via generalized k-Horadam numbers. *Applied Mathematics and Computation, 223*, 191–196.
Zheng, Z. (2022). *Modern cryptography*. Remin University of China.
Zheng, Z., Liu, F., Lu, Y., & Tian, K. (2022). Cyclic lattices, ideal lattices and bounds for the smoothing parameter. *Journal of Information Security, 13*(4), 272–293.
Zheng, Z., Liu, F., Huang, W., Xu, J., & Tian, K. (2022). A generalization of NTRUEncrypt-Cryptosystem based on ideal lattice. *Journal of Information Security, 13*(3), 165–180.