Lattice Based Cryptography for Beginners

– A supplementary note to the following

1. **Peikert's Bonn Lecture Slides**
2. **Lyubashevsky, Peikert and Regev: A toolkit for Ring-LWE**
3. **Steinfeld's Lecture Slides on multilinear maps with Cryptanalysis of GGH map due to Hu and Jia**

Dong Pyo Chi[1,2], Jeong Woon Choi[3], Jeong San Kim[4] and Taewan Kim[5]

[1]*Division of General Studies, UNIST*
dpchi@unist.ac.kr
[2]*Department of Mathematics, Seoul National University*
dpchi@snu.ac.kr
[3]*Fusion Technology R&D Center, SK Telecom*
jw_choi@sk.com
[4]*Department of Applied Mathematics, Kyung Hee University*
freddie1@khu.ac.kr
[5]*Institute of Mathematical Sciences, Ewha Womans University*
aprilsec@ewha.ac.kr

Abstract

The purpose of this lecture note is to introduce lattice based cryptography, which is thought to be a cryptosystem of post-quantum age. We have tried to give as many details possible specially for novice on the subject. Something may be trivial to an expert but not to a novice.

Many fundamental problems about lattice are thought to be hard even against quantum computer, compared to factorization problem which can be solved easily with quantum computer, via the celebrated Shor factorization quantum algorithm. The first part of our presentation is based on slides of Christ Peikert 2013 Bonn lecture (crypt@b-it2013). We, more or less, give somewhat detailed explanation of Professor Peikert's lecture slides. We unfortunately could not attend his Bonn class. We are afraid that there are many mistakes in this note; if any, they are due to our misunderstanding of the material. Part II of our lecture note is on ring LWE, based on the paper "A tool-kit for Ring-LWE Cryptography" by Lyubashevsky, Peikert and Regev. Part III is about multilinear maps together with cryptanalysis of GGH map due to Hu and Jia. Our presentation follows professor Steinfeld's lecture slides on GGHLite, and the paper by Yupu Hu and Huiwen Jia. When you read this lecture note, the corresponding original paper should be accompanied. We thank professor Jung Hee Cheon for introducing the subject and asking Dong Pyo Chi to give a lecture on the subject at the department of mathematics in Seoul National University. We also thank Hyeongkwan Kim for many helps, especially many corrections and improvements of the manuscript during the 2015 Summer session at UNIST. We also thank the students who took the classes at SNU and UNIST. The lecture was given by a novice for novice, so many mistakes are unavoidable. If the reader lets us know any errors, we will very much appreciate it.

Contents

Part I

Lattice Based Cryptography

Chapter 1

Mathematical and Computational Background

1.1 Mathematical Background

In Part I, we use the notations in [P13].

1.1.1 Definitions

Lattice

A lattice $\mathcal{L}$ of $\mathbb{R}^n$ is by definition a discrete subgroup of $\mathbb{R}^n$. In this note we only deal with full-rank lattice, i.e., $\mathcal{L}$ spans $\mathbb{R}^n$ with real coefficients. Moreover, we consider only integer lattices, i.e., $\mathcal{L} \subseteq \mathbb{Z}^n$.

Remark 1.1.1. $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ is not a lattice. Note that when α is irrational, $n\alpha \bmod 1$ is uniformly dense in $S^1 = [0,1]/0 \sim 1$ (Weyl theorem).

Bases

A basis of $\mathcal{L}$ is an ordered set $\mathbb{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ such that

$$\mathcal{L} = \mathcal{L}(\mathbb{B}) = \mathbb{B} \cdot \mathbb{Z}^n = \left\{ \sum_{i=1}^{n} c_i \mathbf{b}_i : c_i \in \mathbb{Z} \right\}. \tag{1.1}$$

Note that by convention, $\mathbf{b}_i$ are column vectors and $\mathbb{B} \cdot \mathbf{k} = k_1\mathbf{b}_1 + \cdots + k_n\mathbf{b}_n$, where $\mathbf{k}$ is a column vector.

Fundamental parallelepiped of basis $\mathbb{B}$ is

$$P(\mathbb{B}) = \mathbb{B} \cdot \left[-\frac{1}{2}, \frac{1}{2}\right)^n \tag{1.2}$$

$$= \left\{ \sum_{i=1}^{n} \alpha_i \mathbf{b}_i : -\frac{1}{2} \leq \alpha_i < \frac{1}{2} \right\}. \tag{1.3}$$

Note that $P(\mathbb{B})$ depends not only on lattice but also on the choice of basis $\mathbb{B}$. A "good" basis of $\mathcal{L}$ gives rather a square-like parallelepiped, while a 'bad' basis gives a very thin parallelepiped. It is trivial to see the following lemma.

Lemma 1.1.2.

$$\mathbb{R}^n = \bigcup_{\mathbf{v}\in\mathcal{L}} (\mathbf{v} + P(\mathbb{B})), \tag{1.4}$$

that is, parallel translation by lattice vectors of parallelepiped covers $\mathbb{R}^n$ without overlap.

Proof. For any $p \in \mathbb{R}^n$,

$$\begin{aligned} p &= \sum_i x_i \mathbf{b}_i & (1.5)\\ &= \sum_i \lceil x_i \rfloor \mathbf{b}_i + \sum_i (x_i - \lceil x_i \rfloor)\mathbf{b}_i, & (1.6)\end{aligned}$$

where $\lceil a \rfloor$ means rounding off. For example, $\lceil 2.7 \rfloor = 3$, $\lceil 2.5 \rfloor = 3$, and $\lceil 2.1 \rfloor = 2$. Therefore,

$$-\frac{1}{2} \le a - \lceil a \rfloor < \frac{1}{2}. \tag{1.7}$$

Hence, $\displaystyle\sum_i \lceil x_i \rfloor \mathbf{b}_i \in \mathcal{L}$ and $\displaystyle\sum_i (x_i - \lceil x_i \rfloor)\mathbf{b}_i \in P(\mathbb{B})$. This shows that $\mathbb{R}^n = \bigcup_{\mathbf{v}\in\mathcal{L}}(\mathbf{v} + P(\mathbb{B}))$.

If $(\mathbf{v}_1 + P(\mathbb{B})) \cap (\mathbf{v}_2 + P(\mathbb{B})) \neq \varnothing$ for some $\mathbf{v}_1 \neq \mathbf{v}_2 \in \mathcal{L}$, then $\mathbf{v}_1 + \alpha = \mathbf{v}_2 + \beta$ for some $\alpha, \beta \in P(\mathbb{B})$, so $\mathbf{v}_1 - \mathbf{v}_2 = \beta - \alpha$. Since $\mathbf{v}_1 - \mathbf{v}_2$ is a $\mathbb{Z}$-linear combination of $\mathbf{b}_i$ while $\beta - \alpha$ is a $(-1, 1)$-linear combination of $\mathbf{b}_i$, so $\mathbf{v}_1 - \mathbf{v}_2 = 0 = \beta - \alpha$.

□

$\mathbb{B}U$ is also basis for any $U \in GL(n : \mathbb{Z})$, i.e., U is an $n \times n$ integer matrix with determinant ± 1. Note that, for example,

$$\begin{pmatrix} 1 & 10^{23} \\ 0 & 1 \end{pmatrix} \in GL(2 : \mathbb{Z}). \tag{1.8}$$

Coset and Determinant

It is much better to think a coset element of $\mathbb{Z}^n/\mathcal{L}$ concretely (note that we assumed $\mathcal{L} \subseteq Z^n$), as a subset $\mathbf{v} + \mathcal{L}$, i.e. a shift of the lattice $\mathcal{L}$, where $\mathbf{v} \in \mathbb{Z}^n$ represents a coset of $\mathbb{Z}^n/\mathcal{L}$.

Lemma 1.1.3. Each coset of $\mathcal{L}$ has a unique representative in a parallelepiped $P(\mathbb{B})$, because $\displaystyle\bigcup_{\mathbf{v}\in\mathcal{L}} (\mathbf{v} + P(\mathbb{B}))$ covers $\mathbb{R}^n$ without overlap.

Proof. Let $\mathbf{v} \in \mathbb{Z}^n$ be a representative of a coset $\mathbf{v} + \mathcal{L}$. Since $\displaystyle\bigcup_{\mathbf{w}\in\mathcal{L}} (\mathbf{w} + P(\mathbb{B}))$ covers $\mathbb{R}^n$ without any overlap, there exists a unique $\mathbf{w} \in \mathcal{L}$ such that $\mathbf{v} \in (\mathbf{w} + P(\mathbb{B}))$. Then $\mathbf{v} - \mathbf{w} \in P(\mathbb{B})$, and $\mathbf{v}$ represents the same coset, i.e.,

$$\mathbf{v} + \mathcal{L} = (\mathbf{v} - \mathbf{w}) + \mathcal{L}, \tag{1.9}$$

so $\mathbf{v} - \mathbf{w}$ is a representative of the coset $\mathbf{v} + \mathcal{L}$ in $P(\mathbb{B})$. Moreover, such a representative is unique, since if $\mathbf{v}_1, \mathbf{v}_2 \in P(\mathbb{B})$ and

$$\mathbf{v}_1 + \mathcal{L} = \mathbf{v}_2 + \mathcal{L}, \tag{1.10}$$

where

$$\begin{aligned}
\mathbf{v}_1 &= \sum c_{1j}\mathbf{b}_j, \qquad -\frac{1}{2} \le c_{1j} < \frac{1}{2}, && (1.11)\\
\mathbf{v}_2 &= \sum c_{2j}\mathbf{b}_j, \qquad -\frac{1}{2} \le c_{2j} < \frac{1}{2}, && (1.12)
\end{aligned}$$

then

$$\mathbf{v}_1 - \mathbf{v}_2 = \sum (c_{1j} - c_{2j})\mathbf{b}_j \in \mathcal{L}, \tag{1.13}$$

i.e., $c_{1j} - c_{2j} \in \mathbb{Z}$ for all j. Note that if $-\frac{1}{2} \le a < \frac{1}{2}$ and $-\frac{1}{2} \le b < \frac{1}{2}$, then then $-1 \lneqq a - b \lneqq 1$. Hence, $c_{1j} - c_{2j} = 0$ for $j = 1, 2, \ldots, n$. $\square$

By definition,

$$\det(\mathcal{L}) := |\mathbb{Z}^n/\mathcal{L}| = |\det \mathbb{B}| = \mathrm{vol}(P(\mathbb{B})) \tag{1.14}$$

for any basis $\mathbb{B}$ of $\mathcal{L}$.

Lemma 1.1.4. $|\mathbb{Z}^n/\mathcal{L}| = \mathrm{vol}(P(\mathbb{B}))$.

Proof. Note the following:

- $\mathcal{L} + P(\mathbb{B})$ covers $\mathbb{R}^n$ without overlap.
- $\mathbb{Z}^n + \boxed{\cdot}$ covers $\mathbb{R}^n$ without overlap, where $\boxed{\cdot}$ means the half closed unit cube $\left[-\frac{1}{2}, \frac{1}{2}\right)^n$.

Thus,

$$\begin{aligned}
\mathcal{L} + P(\mathbb{B}) &= \mathbb{R}^n && (1.15)\\
&= \mathbb{Z}^n + \boxed{\cdot} && (1.16)\\
&= \bigcup_{\mathbf{c} \in \mathbb{Z}^n/\mathcal{L}} (\mathbf{c} + \mathcal{L} + \boxed{\cdot}). && (1.17)
\end{aligned}$$

It follows that $|\mathbb{Z}^n/\mathcal{L}|\,\|\boxed{\cdot}\| = |P(\mathbb{B})|$, so $|\mathbb{Z}^n/\mathcal{L}| = \mathrm{vol}(P(\mathbb{B}))$. $\square$

Successive Minima

Successive minima of linearly independent vectors are defined as follows:

- $\lambda_1(\mathcal{L}) := \min_{0 \ne \mathbf{v} \in \mathcal{L}} \|\mathbf{v}\| = \min_{\mathbf{x} \ne \mathbf{y} \in \mathcal{L}} \|\mathbf{x} - \mathbf{y}\|$
- $\lambda_i(\mathcal{L}) := \min \{r : \mathcal{L} \text{ contains } i \text{ linearly independent vectors of length} \le r\}$.

Then $\lambda_1(\mathcal{L}) \le \lambda_2(\mathcal{L}) \le \cdots \le \lambda_n(\mathcal{L})$. Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ be corresponding lattice elements. Note that $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ need not be a basis of $\mathcal{L}$.

Example 1.1.1. Let $\mathcal{L} \subset \mathbb{Z}^n$ be spanned by $2\mathbf{e}_1, \ldots, 2\mathbf{e}_n, (1, 1, \ldots, 1)$, where $n > 4$. Then $\mathbf{v} = (v_1, \ldots, v_n) \in \mathcal{L}$ if and only if $v_1 = v_2 = \cdots = v_n \mod 2$. Then

$$\lambda_1(\mathcal{L}) = \cdots = \lambda_n(\mathcal{L}) = 2. \tag{1.18}$$

But $\{2\mathbf{e}_1, \ldots, 2\mathbf{e}_n\}$ is not a basis of $\mathcal{L}$. $(1, 1, \ldots, 1)$ or its variation should be an element of any basis of $\mathcal{L}$.

1.1.2 Two simple bounds on the minimum distance

Gram-Schmidt Orthogonalization and Lower Bounding λ_1

The Gram-Schmidt orthogonalization $\widetilde{\mathbb{B}}$ of a basis $\mathbb{B}$ of $\mathcal{L}$ is given by

$$\begin{aligned}
\mathbb{B} &= QR && (1.19)\\
&= Q\begin{pmatrix} \|\widetilde{\mathbf{b}_1}\| & & * \\ & \ddots & \\ 0 & & \|\widetilde{\mathbf{b}_n}\| \end{pmatrix} && (1.20)\\
&= \widetilde{\mathbb{B}}\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}, && (1.21)
\end{aligned}$$

where

$$\widetilde{\mathbb{B}} = Q\begin{pmatrix} \|\widetilde{\mathbf{b}_1}\| & & 0 \\ & \ddots & \\ 0 & & \|\widetilde{\mathbf{b}_n}\| \end{pmatrix},$$

and Q is an orthonormal basis reduced from $\widetilde{\mathbb{B}}$, and R is a representation of $\mathbb{B}$ with respect to this basis.

Lemma 1.1.5. $P(\widetilde{\mathbb{B}}) = \widetilde{\mathbb{B}} \cdot \left[-\frac{1}{2}, \frac{1}{2}\right)^n$ is a fundamental domain of $\mathcal{L}$. That is, $\mathcal{L} + P(\widetilde{\mathbb{B}})$ covers $\mathbb{R}^n$ without overlap.

Proof. Since $\mathrm{vol}(P(\widetilde{\mathbb{B}})) = \mathrm{vol}(P(\mathbb{B}))$, it suffices to show that there is no overlap. Assume there is a overlap, i.e.,

$$\mathbb{B}\mathbf{x} + \widetilde{\mathbb{B}}\alpha = \mathbb{B}\mathbf{y} + \widetilde{\mathbb{B}}\beta \tag{1.22}$$

for some $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$ and $\vec{\alpha}, \vec{\beta} \in \left[-\frac{1}{2}, \frac{1}{2}\right)^n$. Then $\mathbb{B}(\mathbf{x} - \mathbf{y}) = \widetilde{\mathbb{B}}(\vec{\beta} - \vec{\alpha})$. Letting $\mathbf{z} = \mathbf{x} - \mathbf{y}$,

$$\widetilde{\mathbb{B}}\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}\mathbf{z} = \widetilde{\mathbb{B}}(\vec{\beta} - \vec{\alpha}), \tag{1.23}$$

so

$$\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}\mathbf{z} = (\vec{\beta} - \vec{\alpha}). \tag{1.24}$$

Note that $\mathbf{z}$ is an integer vector and

$$-1 \lneqq \beta_i - \alpha_i \lneqq 1. \tag{1.25}$$

From the equality (1.24),

$$\begin{aligned}
z_n &= \beta_n - \alpha_n \quad \therefore z_n = 0 \to \alpha_n = \beta_n && (1.26)\\
z_{n-1} + *z_n &= \beta_{n-1} - \alpha_{n-1} && (1.27)\\
z_{n-1} &= \beta_{n-1} - \alpha_{n-1} \quad \therefore z_{n-1} = 0 \to \alpha_{n-1} = \beta_{n-1} && (1.28)\\
&\cdots &&\\
\therefore z_1 &= 0 && (1.29)\\
\text{i.e., } \mathbf{x} &= \mathbf{y}. && (1.30)
\end{aligned}$$

□

It is easy to see that $\lambda_1(\mathcal{L}) \geq \min_i \|\widetilde{\mathbf{b}_i}\|$ from $\mathbb{B}\mathbf{c} = Q(R\mathbf{c})$ for $\mathbf{c} \in \mathbb{Z}^n$.

Upper Bounding λ_1: Minkowski's Theorem

Theorem 1.1.6 (Minkowski Theorem 1)**.** Any convex centrally symmetric body S of volume $> 2^n \det(\mathcal{L})$ contains a nonzero lattice point.

Proof. Let $S' = \frac{1}{2}S$, so $\mathrm{vol}(S') > \det(\mathcal{L})$. Then there exist $\mathbf{x} \neq \mathbf{y} \in S'$ such that $\mathbf{x} - \mathbf{y} \in \mathcal{L}$, since for some $\mathbf{v}_1 \neq \mathbf{v}_2 \in \mathcal{L}$,

$$(\mathbf{v}_1 + S') \bigcap (\mathbf{v}_2 + S') \neq \phi \tag{1.31}$$

$$\mathbf{z} = \mathbf{v}_1 + \mathbf{x} = \mathbf{v}_2 + \mathbf{y}, \quad \mathbf{x}, \mathbf{y} \in S' \tag{1.32}$$

$$\mathbf{x} - \mathbf{y} = \mathbf{v}_2 - \mathbf{v}_1 \neq 0 \in \mathcal{L}. \tag{1.33}$$

Now $2\mathbf{x}, -2\mathbf{y} \in S$ by the definition of S', so

$$\mathbf{x} - \mathbf{y} = \frac{1}{2}(2\mathbf{x}) + \frac{1}{2}(-2\mathbf{y}) \in S$$

by the convexity of S. □

Corollary 1.1.7.

$$\lambda_1(\mathcal{L}) \leq \sqrt{n}(\det \mathcal{L})^{\frac{1}{n}}. \tag{1.34}$$

Proof. We give a proof of the corollary using the following two facts:

- A ball of radius $> \sqrt{n}(\det \mathcal{L})^{\frac{1}{n}}$ is convex and centrally symmetric.
- $B(0, \sqrt{n}(\det \mathcal{L})^{\frac{1}{n}}) \supset$ a cube of side length $2(\det \mathcal{L})^{\frac{1}{n}}$, since

$$\mathrm{dist}\left((1, \ldots, 1), (0, \ldots, 0)\right) = \sqrt{n}.$$

It follows that

$$\mathrm{vol}(B(0, \sqrt{n}(\det \mathcal{L})^{\frac{1}{n}})) > 2^n \det \mathcal{L}.$$

□

Remark 1.1.8. We could obtain a more refined inequality if we use the exact formula for $\mathrm{vol}(B(0, R))$. Choose R such that $\mathrm{vol}(B(0, R)) = 2^n \det \mathcal{L}$. Then $\lambda_1(\mathcal{L}) \leq R$.

Theorem 1.1.9 (Minkowski Theorem 2)**.** $(\prod_{i=1}^n \lambda_i(\mathcal{L}))^{\frac{1}{n}} \leq \sqrt{n}(\det \mathcal{L})^{\frac{1}{n}}$.

Proof. We may assume $\|\mathbf{b}_i\| = \lambda_i(\mathcal{L})$ for $i = 1, \ldots, n$, and consider a lattice generated by $\mathbf{b}_1, \ldots, \mathbf{b}_n$, possibly a sublattice of $\mathcal{L}$.

$$T := \left\{ \mathbf{y} \in \mathbb{R}^n : \sum_{i=1}^n \left(\frac{\left\langle \mathbf{y}, \widetilde{\mathbf{b}_i} \right\rangle}{\|\widetilde{\mathbf{b}_i}\| \lambda_i} \right)^2 < 1 \right\}. \tag{1.35}$$

<u>Claim:</u> The ellipsoid T does not contain any nonzero lattice point.
Let $0 \neq \mathbf{y} \in \mathcal{L}$, and $1 \leq k \leq n$ maximal such that

$$\lambda_{k+1}(\mathcal{L}) \gneqq \|\mathbf{y}\| \geq \lambda_k(\mathcal{L}). \tag{1.36}$$

We claim $\mathbf{y} \in \operatorname{span}\{\mathbf{b}_1, \ldots, \mathbf{b}_k\} = \operatorname{span}\{\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_k\}$. If not, $\mathbf{b}_1, \ldots, \mathbf{b}_k, \mathbf{y}$ are $k+1$ linearly independent and their norms are less than λ_{k+1}, a contradiction. Hence,

$$\sum_{i=1}^{n} \left(\frac{\left\langle \mathbf{y}, \tilde{\mathbf{b}}_i \right\rangle}{\|\tilde{\mathbf{b}}_i\| \lambda_i} \right)^2 = \sum_{i=1}^{k} \left(\frac{\left\langle \mathbf{y}, \tilde{\mathbf{b}}_i \right\rangle}{\|\tilde{\mathbf{b}}_i\| \lambda_i} \right)^2 \tag{1.37}$$

$$\geq \sum_{i=1}^{k} \frac{1}{\lambda_k^2} \left(\frac{\left\langle \mathbf{y}, \tilde{\mathbf{b}}_i \right\rangle}{\|\tilde{\mathbf{b}}_i\|} \right)^2 \tag{1.38}$$

$$= \frac{\|\mathbf{y}\|^2}{\lambda_k^2} \geq 1, \tag{1.39}$$

so $\mathbf{y} \notin T$, i.e., T does not contain any nonzero lattice vector. Hence,

$$2^n \det(\mathcal{L}) \geq \operatorname{vol}(T) = \left(\prod_{i=1}^{n} \lambda_i \right) \operatorname{vol}(B(0:1)) \geq \left(\prod_{i=1}^{n} \lambda_i \right) \left(\frac{2}{\sqrt{n}} \right)^n, \tag{1.40}$$

so

$$\left(\prod_{i=1}^{n} \lambda_i \right)^{\frac{1}{n}} \leq \sqrt{n} (\det \mathcal{L})^{\frac{1}{n}}. \tag{1.41}$$

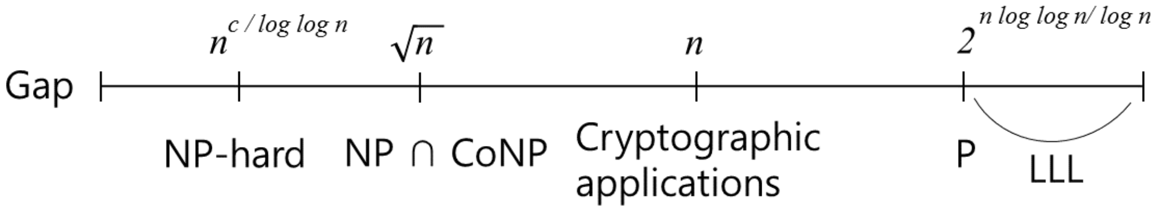
□

1.2 Computational Background

1.2.1 Hard problems

Shortest Vector Problem (SVP)

- SVP_γ: Given a basis $\mathbb{B}$ of $\mathcal{L}$, find nonzero $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v}\| \leq \gamma \lambda_1(\mathcal{L})$.
  There exists an exact algorithm for finding a nonzero minimum vector in time $2^{\mathcal{O}(n)}$, polynomial time algorithm for gap 2^n, but no quantum algorithm with exponential boost.



- $GapSVP_\gamma$: Given a basis $\mathbb{B}$ of $\mathcal{L}$ and a real d, decide between $\lambda_1(\mathcal{L}) \leq d$ and $\lambda_1(\mathcal{L}) > \gamma d$.

Note that $GapSVP_\gamma \leq SVP_\gamma$, i.e., $GapSVP_\gamma$ reduces to SVP_γ. ($SVP_\gamma \to$ find $\mathbf{v} \neq 0 \in \mathcal{L}$ such that $\lambda_1(\mathcal{L}) \leq \|\mathbf{v}\| \leq \gamma\lambda_1(\mathcal{L})$.) If $\|\mathbf{v}\| \leq \gamma d$, then $\lambda_1 \leq \gamma d$. Hence, $\lambda_1 < d$ (because either $\lambda_1 \leq d$ or $\lambda_1 > \gamma d$). If $\|\mathbf{v}\| > \gamma d$, then $\gamma d < \|\mathbf{v}\| \leq \gamma\lambda_1$, so $d < \lambda_1$, hence $\lambda_1 > \gamma d$.) But the reverse direction is open.

LLL (Lenstra-Lenstra-Lovaz) algorithm

$\mathbb{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is a $\delta - LLL$ reduced basis if

(i) For $1 \leq j < i \leq n$, we have $|\mu_{i,j}| \leq \frac{1}{2}$.

(ii) For $1 \leq i < n$, we have

$$\delta \|\tilde{\mathbf{b}}_i\|^2 \leq \|\mu_{i+1,i}\tilde{\mathbf{b}}_i + \tilde{\mathbf{b}}_{i+1}\|^2 = |\mu_{i+1,i}|^2 \|\tilde{\mathbf{b}}_i\|^2 + \|\tilde{\mathbf{b}}_{i+1}\|^2, \tag{1.42}$$

where

$$\mu_{i,j} = \frac{\left\langle \mathbf{b}_i, \tilde{\mathbf{b}}_j \right\rangle}{\|\tilde{\mathbf{b}}_j\|^2}, \tag{1.43}$$

$$\tilde{\mathbf{b}}_i = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \tilde{\mathbf{b}}_j. \tag{1.44}$$

$\mathbb{B}$ has the following form with respect to the orthonormal basis

$$\begin{pmatrix} \|\tilde{\mathbf{b}}_1\| & \mu_{2,1}\|\tilde{\mathbf{b}}_1\| & \mu_{3,1}\|\tilde{\mathbf{b}}_1\| & * & \leq \frac{1}{2}\|\tilde{\mathbf{b}}_1\| \\ & \|\tilde{\mathbf{b}}_2\| & \mu_{3,2}\|\tilde{\mathbf{b}}_1\| & * & \leq \frac{1}{2}\|\tilde{\mathbf{b}}_2\| \\ & & \ddots & & \vdots \\ & & & & \leq \frac{1}{2}\|\tilde{\mathbf{b}}_{n-1}\| \\ & & & & \|\tilde{\mathbf{b}}_n\| \end{pmatrix} \tag{1.45}$$

In particular, if $1 \geq \delta > \frac{1}{4}$, then

$$\|\tilde{\mathbf{b}}_{i+1}\|^2 \geq \left(\delta - \frac{1}{4}\right) \|\tilde{\mathbf{b}}_i\|^2. \tag{1.46}$$

Hence,

$$\|\mathbf{b}_1\| = \|\tilde{\mathbf{b}}_1\| \leq 2^{(n-1)/2} \min \|\tilde{\mathbf{b}}_i\| \leq 2^{(n-1)/2} \lambda_1(\mathcal{L}).$$

(We choose $\delta = \frac{3}{4}$.)

LLL-algorithm

- Input: Lattice basis $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}^n$.
- Output: δ-LLL reduced basis of $\mathcal{L}$.
- Start: compute the Gram-Schmidt Orthogonalization $\tilde{\mathbf{b}}_1, \tilde{\mathbf{b}}_2, \ldots, \tilde{\mathbf{b}}_n$.
- Reduction Step:
  for $i = 2$ to n do
  for $j = i - 1$ to 1 do
  $$\mathbf{b}_i \leftarrow \mathbf{b}_i - c_{ij}\mathbf{b}_j, \quad \text{where } c_{ij} = \left\lceil \frac{\langle \mathbf{b}_i, \tilde{\mathbf{b}}_j \rangle}{\langle \tilde{\mathbf{b}}_j \cdot \tilde{\mathbf{b}}_j \rangle} \right\rfloor.$$
- Swap Step:
  If $\exists\ i$ such that $\delta \|\tilde{\mathbf{b}}_i\|^2 > \|\mu_{i+1,i}\tilde{\mathbf{b}}_i + \tilde{\mathbf{b}}_{i+1}\|^2$
  $\mathbf{b}_i \leftrightarrow \mathbf{b}_{i+1}$
  goto start.
- Output: $\mathbf{b}_1, \ldots, \mathbf{b}_n$.

Shortest Independent Vectors Problem ($SIVP_\gamma$)

Given a basis $\mathbb{B}$, find linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathcal{L}$ such that $\|\mathbf{v}_i\| \leq \gamma\lambda_n(\mathcal{L})$.

Bounded-Distance Decoding (BDD)

Given a basis $\mathbb{B}$, $\vec{t} \in \mathbb{R}^n$, and real $d < \lambda_1/2$ such that $\mathrm{dist}(\vec{t}, \mathcal{L}) \leq d$, find the unique $\mathbf{v} \in \mathcal{L}$ closest to $\vec{t}$. BDD is equivalent to finding $e \in \vec{t} + \mathcal{L}$ such that $\|e\| \leq d$.

Algorithms for BDD

1. Babai's Round off algorithm for BDD
   Using a good basis $\mathbb{B}$,
   $$\vec{t} = \sum \alpha_i \mathbf{b}_i \rightarrow \mathbf{e} := \sum (\alpha_i - \lceil \alpha_i \rfloor)\mathbf{b}_i. \tag{1.47}$$
   It works if $Ball(d) \subseteq P(\mathbb{B})$. Hence, $d \leq min\|\mathbf{b}_i^\perp\|/2$, where $\mathbf{b}_i^\perp$ is the orthogonal component of $\mathbf{b}_i$ to the hyperplane $\mathrm{span}\{\mathbf{b}_1, \cdots, \hat{\mathbf{b}}_i, \cdots, \mathbf{b}_n\}$.

2. Babai's nearest plane algorithm for BDD
   Output $\mathbf{e} = \vec{t} \bmod \widetilde{\mathbb{B}}$, where $\mathbf{e} \in P(\widetilde{\mathbb{B}})$.
   It works if $Ball(d) \subseteq P(\widetilde{\mathbb{B}})$, where $\widetilde{\mathbb{B}}$ is the Gram-Schmidt Orthogonalization of $\mathbb{B}$ as before,
   $$i.e.,\ d \leq \min_i \|\widetilde{\mathbf{b}_i}\|/2. \tag{1.48}$$
   Note that $P(\widetilde{\mathbb{B}})$ is also a fundamental domain of the lattice $\mathcal{L}$.

Chapter 2

Short Integer Solution and Learning With Errors

2.1 Hard problems

2.1.1 Short Integer Solution

Short Integer Solution (SIS)

$\mathbb{Z}_q^n$:= n-dimensional vectors modulo q. Given $\vec{a_1}, \ldots, \vec{a_m} \in \mathbb{Z}_q^n$, find nontrivial and small $z_1, \ldots, z_m \in \mathbb{Z}$ such that

$$z_1\vec{a_1} + \cdots + z_m\vec{a_m} = 0 \tag{2.1}$$

in $\mathbb{Z}_q^n$, i.e.,

$$A\mathbf{z} = 0 \mod q, \tag{2.2}$$

where $A = (\vec{a}_1, \ldots, \vec{a}_m)$. This is finding a short vector in the lattice

$$\begin{aligned} \mathcal{L}(A)^\perp &:= \ker\left(\mathbb{Z}^m \xrightarrow[\mathbf{z}\mapsto A\mathbf{z}]{A\in\mathbb{Z}_q^{n\times m}} \mathbb{Z}_q^n \right) \\ &= \{\mathbf{x} \in \mathbb{Z}^m : A\mathbf{x} = \mathbf{u} \mod q\}. \end{aligned}$$

One-way Hash Function

Set $m > n \log q$. Define $f_A : \{0,1\}^m \to \mathbb{Z}_q^n$ as

$$f_A(\mathbf{x}) = A\mathbf{x}. \tag{2.3}$$

Then f_A covers Z_q^n almost uniformly. (Note that since $m > n \log q$, the number of elements in the domain, 2^m, is much larger than the number of elements in the range, q^n.)

We say collision $\mathbf{x}, \mathbf{x}' \in \{0,1\}^m$ when $A\mathbf{x} = A\mathbf{x}'$.

- $A = (\vec{a_1}, \ldots, \vec{a_m}) \in \mathbb{Z}_q^{n\times m}$ defines a q-ary lattice

$$\mathcal{L}^\perp(A) = \{\mathbf{z} \in \mathbb{Z}^m : A\mathbf{z} = 0 \mod q\}.$$

- Hence, SIS is SVP on $\mathcal{L}^\perp(A)$.

- A syndrome $\mathbf{u} \in \mathbb{Z}_q^n$ defines a coset
$$\mathcal{L}_{\mathbf{u}}^{\perp}(A) = \{\mathbf{x} \in \mathbb{Z}^m : A\mathbf{x} = \mathbf{u} \mod q\}$$
of $\mathcal{L}^{\perp}(A)$.

Remark 2.1.1. We are assuming that A has n-linearly independent columns. Hence, $A : \mathbb{Z}^m \to \mathbb{Z}_q^n$ is onto, so $|\mathbb{Z}^m/\mathcal{L}^{\perp}(A)| = q^n$, i.e., $\det \mathcal{L}^{\perp}(A) = q^n$.

Worst-Case / Average-Case reduction

Finding a short nonzero $z \in \mathcal{L}^{\perp}(A)$ for uniformly random $A \in \mathbb{Z}_q^{n\times m}$, where $m \approx n \ln q$ $\Rightarrow$ Solving $GapSVP_{\beta\sqrt{n}}$, $SIVP_{\beta\sqrt{n}}$ on any n-dimensional lattice.

Algorithm for reduction

Repeat m-times.
  Pick a random lattice point $\mathbf{v}_i \in \mathcal{L}$, where $\mathcal{L}$ is an n-dimensional lattice.
  Gaussian sample a point in $\frac{1}{q}\mathcal{L}$ around the lattice point $\mathbf{v}_i \in \mathcal{L}$.
Hence, each sampled point can be written as $\mathbf{v}_i + \frac{1}{q}\mathbb{B}\vec{a_i}$, where $\frac{1}{q}\mathbb{B}\vec{a_i}$ is short.
Give the m $\mathbb{Z}_q^n$ samples $\vec{a_1}, \ldots, \vec{a_m}$ to SIS oracle. Note that
$$A = (\vec{a}_1, \ldots, \vec{a}_n) \in \mathbb{Z}_q^{n\times m}$$
is uniform. We subdivided the sides of the given lattice by "q". So each lattice domain of $\mathcal{L}$ has q^n subpoints inside.

SIS oracle outputs $z_1, \ldots, z_m \in \{-1, 0, 1\}$ such that
$$z_1\vec{a_1} + \cdots + z_m\vec{a_m} = 0 \pmod q. \tag{2.4}$$
Therefore, $\sum z_i(\mathbf{v}_i + \frac{1}{q}\mathbb{B}\vec{a_i})$ is a lattice point of the given lattice $\mathcal{L}$. Hence,
$$\frac{1}{q}\mathbb{B}(z_1\vec{a_1} + \cdots + z_m\vec{a_m}) \tag{2.5}$$
is a short lattice vector in $\mathcal{L}$ since it is the sum of short vectors $\frac{1}{q}\mathbb{B}\vec{a_i}$.

2.1.2 Learning With Errors

Learning With Errors (LWE)

- Search LWE: Find $\mathbf{s} \in \mathbb{Z}_q^n$ given noisy random inner products
$$\vec{a_1} \leftarrow \mathbb{Z}_q^n, \qquad b_1 = \langle \mathbf{s}, \vec{a_1}\rangle + e_1 \tag{2.6}$$
$$\vec{a_2} \leftarrow \mathbb{Z}_q^n, \qquad b_2 = \langle \mathbf{s}, \vec{a_2}\rangle + e_2 \tag{2.7}$$
$$\vdots$$
where $e_i \leftarrow \chi$, χ Gaussian over $\mathbb{Z}$ with width αq. ($\alpha q > \sqrt{n}$)
$$\mathbb{Z}_q^n \times \mathbb{Z}^m \xrightarrow[(\mathbf{s},\mathbf{e})\mapsto \mathbf{s}^t A+\mathbf{e}]{A\in\mathbb{Z}_q^{n\times m}} \mathbb{Z}_q^m$$
- Decision LWE: Distinguish $(A,\ \mathbf{b}^t = \mathbf{s}^t A + e^t)$ from uniform $(A,\ \mathbf{b}^t)$, where $A = (\vec{a_1}, \ldots, \vec{a_m})$.

Note that Search LWE $\Leftrightarrow$ Decision LWE.

Lattice interpretation of LWE

$$\mathcal{L}(A) := \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{z}^t = \mathbf{s}^t A \mod q \text{ for some } \mathbf{s} \in \mathbb{Z}_q^n\} = \pi^{-1}(\operatorname{im} A)$$

$$\begin{tikzcd}
 & \mathbb{Z}^m \arrow[d, "\pi"] \\
\mathbb{Z}_q^n \arrow[r, "A", "\mathbf{s} \mapsto \mathbf{s}^t A"'] & \mathbb{Z}_q^m
\end{tikzcd}$$

Then, LWE $\Leftrightarrow$ BDD on $\mathcal{L}(A)$. (Remark: From $\mathbf{z}^t = \mathbf{s}^t A + \mathbf{e}$, we obtain $\mathbf{z}^t$ by BDD, then solve the simultaneous equation $\mathbf{z}^t = \mathbf{s}^t A \mod q$ to obtain $\mathbf{s}$.)

SIS versus LWE

- Regev: LWE $\geq$ GapSVP, SIVP quantumly. (Peikert *et al.* showed LWE $\geq$ GapSVP classically. But, classical reduction LWE $\geq$ SVP, or LWE $\geq$ SIVP is unknown.)
- SIS $\geq$ LWE:
  If we find short $\mathbf{z}$ such that $A\mathbf{z} = 0$, then from $\mathbf{b}^t = \mathbf{s}^t A + e^t$, we find $\mathbf{b}^t\mathbf{z} = 0 + e^t\mathbf{z}$; if $(A,\ \mathbf{b}^t)$ is LWE, then $\mathbf{b}^t\mathbb{Z}$ is short; if $(A,\ \mathbf{b}^t)$ is not LWE, then $\mathbf{b}^t\mathbf{z}$ rather well spread.
- SIS $\leq$ LWE quantumly.

Simple properties of LWE

1. Easy to check a candidate solution $\mathbf{s}' \in \mathbb{Z}_q^n$: test if $\mathbf{b} - \langle \mathbf{s}', \vec{a} \rangle$ is small.
   If $\mathbf{s} \neq \mathbf{s}'$, then $\mathbf{b} - \langle \mathbf{s}', \vec{a} \rangle = \langle \mathbf{s} - \mathbf{s}', \vec{a} \rangle + e$ is well spread in $\mathbb{Z}_q$.
2. Shift the secret by any $\mathbf{t} \in \mathbb{Z}_q^n$,

$$(\vec{a}, b = \langle \mathbf{s}, \vec{a} \rangle + e) \to (\vec{a}, b' = b + \langle \mathbf{t}, \vec{a} \rangle = \langle \mathbf{s} + \mathbf{t}, \vec{a} \rangle + e). \tag{2.8}$$

   random $\mathbf{t}$s $\to$ random self-reduction.
   We obtain many new LWEs with essentially the same solutions. Hence, we can boost success probabilities arbitrarily close to 1.

Proof of equivalence of Search/Decision of LWE.

Suppose that $\mathcal{D}$ solves decision-LWE, i.e., it perfectly distinguish between $(\vec{a}, b = \langle \mathbf{s}, \vec{a} \rangle + e)$ and uniform $(\vec{a}, b)$. We want to solve search LWE; i.e., given pairs $(\vec{a}, b)$, find $\mathbf{s}$. To find $s_1 \in \mathbb{Z}_q$, it suffices to test whether $s_1 = 0$ because we can shift s_1 by $0, 1, \ldots, q-1$, i.e., choose $\mathbf{t} = (0, 0, \ldots, 0)$ or $\mathbf{t} = (1, 0, \ldots, 0), \mathbf{t} = (2, 0, \ldots, 0), \ldots, \mathbf{t} = (q-1, 0, \ldots, 0)$. For each $(\vec{a}, b)$, choose $r \leftarrow \mathbb{Z}_q$. Invoke $\mathcal{D}$ on pairs $(\vec{a'} = \vec{a} - (r, 0, \ldots, 0), b)$. Since

$$\begin{aligned}
b &= \langle \mathbf{s}, \vec{a} \rangle + e \\
&= \left\langle \mathbf{s}, \vec{a'} + (r, 0, \ldots, 0) \right\rangle + e \\
&= \left\langle \mathbf{s}, \vec{a'} \right\rangle + s_1 r + e,
\end{aligned}$$

we see that if $s_1 = 0$, then $b = \left\langle \mathbf{s}, \vec{a'} \right\rangle + e$ is LWE, and if $s_1 \neq 0$, then b is uniform.

Decision-LWE with 'Short' Secret

We may assume that the secret is short, i.e., drawn from the error distribution χ^n. In this case, we say that our LWE is in Hermite Normal Form (HNF of LWE).

1. Draw samples to get $(\bar{A}, \bar{\mathbf{b}}^t = \mathbf{s}^t\bar{A} + \bar{\mathbf{e}}^t)$ for square invertible $\bar{A}$.

2. Transform additional samples of LWE $(\vec{a}, b = \langle \mathbf{s}, \vec{a}\rangle + e)$ to $\vec{a'} = -\bar{A}^{-1}\vec{a}$,

$$\begin{aligned}
b' &= b + \left\langle \bar{\mathbf{b}}, \vec{a'} \right\rangle \\
&= \langle \mathbf{s}, \vec{a}\rangle + e + \left\langle \bar{A}^t\mathbf{s} + \bar{\mathbf{e}}, \vec{a'} \right\rangle \\
&= \langle \mathbf{s}, \vec{a}\rangle + \left\langle \bar{A}^t\mathbf{s}, \vec{a'} \right\rangle + \left\langle \bar{\mathbf{e}}, \vec{a'} \right\rangle + e \\
&= \langle \mathbf{s}, \vec{a}\rangle + \langle \mathbf{s}, \bar{A}(-\bar{A}^{-1})\vec{a}\rangle + \left\langle \bar{\mathbf{e}}, \vec{a'} \right\rangle + e \\
&= \left\langle \bar{\mathbf{e}}, \vec{a'} \right\rangle + e.
\end{aligned}$$

$(\vec{a'}, b')$ is LWE with secret $\bar{\mathbf{e}}$. Then we obtain $\mathbf{s}$ from $\bar{\mathbf{b}}^t = \mathbf{s}^t\bar{A} + \bar{\mathbf{e}}^t$.

2.2 Cryptosystems

2.2.1 Public-Key Cryptosystem using LWE

(Due to Regev)
$A \leftarrow \mathbb{Z}_q^{n\times m}$ (i.e., uniformly random $n \times m$ matrix over $\mathbb{Z}_q$) open public.
$\mathbf{s} \leftarrow \mathbb{Z}_q^n$ Alice secret.
Public key of Alice

$$\mathbf{b}^t = \mathbf{s}^t A + \mathbf{e}^t. \tag{2.9}$$

$\mathbf{x} \leftarrow \{0,1\}^m$ Bob secret.
Bob sends to Alice

$$\begin{aligned}
\mathbf{u} &= A\mathbf{x}, &(2.10)\\
\mathbf{u}' &= \mathbf{b}^t\mathbf{x} + bit \cdot q/2. &(2.11)
\end{aligned}$$

Alice decodes $\mathbf{u}' - \mathbf{s}^t\mathbf{u} \approx bit \cdot q/2$.
Note that $(A, \mathbf{b}^t)$ is LWE and $(\mathbf{u}, \mathbf{u}')$ uniformly random by left-over hash lemma when $m \geq n \log q$.

2.2.2 Dual cryptosystem

$A \leftarrow \mathbb{Z}_q^{n\times m}$ open public as before.
Alice chooses a secret $\mathbf{x} \leftarrow \{0,1\}^m$.
Alice's public key

$$\mathbf{u} = A\mathbf{x}. \tag{2.12}$$

(by LHL, uniform if $m \geq n \log q$.)
Bob chooses a secret $\mathbf{s} \leftarrow \mathbb{Z}_q^n$.
Bob sends

$$\begin{aligned}\mathbf{b}^t &= \mathbf{s}^t A + \mathbf{e}^t, && (2.13)\\ b' &= \mathbf{s}^t \mathbf{u} + e' + bit \cdot q/2. && (2.14)\end{aligned}$$

Adding $bit \cdot q/2$ does not change the uniformity of $\mathbf{s}^t A + \mathbf{e}^t$.
Alice decodes $b' - \mathbf{b}^t \mathbf{x} \approx bit \cdot q/2$.
Note that $(A, \mathbf{u}; \mathbf{b}, b')$ is a LWE pair.

2.2.3 More efficient Cryptosystem

$A \leftarrow \mathbb{Z}_q^{n \times n}$ open public.
Alice chooses a secret $\mathbf{s} \leftarrow \chi^n$ and an error $\mathbf{e} \leftarrow \chi^n$.
Alice's public key

$$\mathbf{u}^t = \mathbf{s}^t A + \mathbf{e}^t. \qquad (2.15)$$

Bob chooses a secret $\mathbf{r} \leftarrow \chi^n, x \leftarrow \chi$, and $\mathbf{x}, x' \in \chi$.
Bob sends

$$\begin{aligned}\mathbf{b} &= A\mathbf{r} + \mathbf{x} && (2.16)\\ b' &= \mathbf{u}^t \mathbf{r} + x' + bit \cdot q/2. && (2.17)\end{aligned}$$

Alice decodes $b' - \mathbf{s}^t \mathbf{b} \approx bit \cdot q/2$.
Note that $(A, \mathbf{u}; \mathbf{b}, b')$ is a Hermite normal form of LWE.

Chapter 3

Discrete Gaussians and Applications

3.1 Discrete Gaussians and sampling

3.1.1 Discrete Gaussians

Gaussian sampling

Define
$$\rho_s(x) := \exp\left(-\frac{\pi\|x\|^2}{s^2}\right). \tag{3.1}$$
Note that ρ_s is rather flat if s is large, and steep if s is small.

Note that
$$\int_{x\in\mathbb{R}^n} \rho_s(x)dx = s^n. \tag{3.2}$$
Hence, $v_s := \frac{\rho_s}{s^n}$ is an n-dimensional Gaussian probability density. We define Fourier Transform as
$$\hat{h}(w) = \int_{\mathbb{R}^n} h(x)e^{-2\pi i\langle x,w\rangle}dx. \tag{3.3}$$

Hence,

$$\begin{aligned}
\hat{\rho}_s(y) &= \int_{\mathbb{R}^n} \rho_s(x)e^{-2\pi i x\cdot y}dx && (3.4)\\
&= \int_{\mathbb{R}^n} e^{-\pi\left(\frac{\|x\|^2}{s^2}+2ix\cdot y\right)}dx && (3.5)\\
&= \int_{\mathbb{R}^n} e^{-\pi\sum_i\left(\frac{x_i}{s}+iy_i s\right)^2}e^{-\pi(\|y\|s)^2}dx && (3.6)\\
&= s^n\rho_{\frac{1}{s}}(y). && (3.7)
\end{aligned}$$

Hence, if $\rho_s(x)$ rather steep, then $\hat{\rho_s}$ is rather flat, and vice versa.

Remark 3.1.1.

$$\begin{aligned}
\int_{\mathbb{R}} e^{-\pi x^2}dx &= 1, && (3.8)\\
\int_{\mathbb{R}} e^{-\pi\left(\frac{x}{s}\right)^2}dx &= s. && (3.9)
\end{aligned}$$

Poisson summation formula

Let

$$f(x) : \mathbb{R} \to \mathbb{C} \tag{3.10}$$
$$F(\theta) := \sum_{n\in\mathbb{Z}} f(\theta+n) : S^1 \to \mathbb{C}, \tag{3.11}$$

where $S^1 = [0,1]/0 \sim 1$. Then the Fourier series of $F(\theta)$ is

$$F(\theta) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi i n\theta}, \tag{3.12}$$

where

$$\begin{aligned}
a_n &= \int_0^1 F(\theta) e^{-2\pi i n\theta} d\theta && (3.13)\\
&= \int_0^1 \left(\sum_k f(\theta+k)\right) e^{-2\pi i n\theta} d\theta && (3.14)\\
&= \int_{-\infty}^{\infty} f(\theta) e^{-2\pi i n\theta} d\theta && (3.15)\\
&= \hat{f}(n), && (3.16)
\end{aligned}$$

i.e., $F(\theta) = \sum \hat{f}(n) e^{2\pi i n\theta}$.
In particular, we obtain Poisson Summation Formula

$$F(0) = \sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n). \tag{3.17}$$

In general, for $h : \mathbb{R}^n \to \mathbb{C}$,

$$\hat{h}(\mathbb{Z}^n) = h(\mathbb{Z}^n). \tag{3.18}$$

Generalized Poisson summation formula

Let $f : \mathbb{R}^n \to \mathbb{C}$.

$$f(L) = \det L^* \hat{f}(L^*), \tag{3.19}$$

where $L \subset \mathbb{Z}^n$ is a lattice and

$$L^* = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x}\cdot\mathbf{y} \in \mathbb{Z}, \quad \forall \mathbf{y} \in L\} \tag{3.20}$$

is called the dual lattice of L.

Proof. Let $L = A\mathbb{Z}^n$ for some $n \times n$ matrix A.

$$\begin{aligned}
f(L) &= (f \circ A)(\mathbb{Z}^n) && (3.21)\\
&= \widehat{(f \circ A)}(\mathbb{Z}^n) && (3.22)
\end{aligned}$$

by Poisson summation formula. Let's compute

$$\begin{aligned}
\widehat{f \circ A}(\mathbf{y}) &= \int_{\mathbb{R}^n} e^{-2\pi i\langle \mathbf{x},\mathbf{y}\rangle}(f \circ A)(\mathbf{x})d\mathbf{x} && (3.23)\\
&\quad \text{putting} \quad A\mathbf{x} =: \mathbf{x}' \\
&= \frac{1}{\det A}\int_{\mathbb{R}^n} e^{-2\pi i\left\langle A^{-1}\mathbf{x}',\mathbf{y}\right\rangle} f(\mathbf{x}')d\mathbf{x}' && (3.24)\\
&= \frac{1}{\det A}\int_{\mathbb{R}^n} e^{-2\pi i\left\langle \mathbf{x}',A^{-1^T}\mathbf{y}\right\rangle} f(\mathbf{x}')d\mathbf{x}' && (3.25)\\
&= \frac{1}{\det A}\cdot \hat{f}(A^{-T}\mathbf{y}). && (3.26)
\end{aligned}$$

Hence,

$$\begin{aligned}
\widehat{f \circ A}(\mathbb{Z}^n) &= \frac{1}{\det A}\hat{f}(A^{-T}\mathbb{Z}^n) && (3.27)\\
&= \det \mathcal{L}^* \hat{f}(\mathcal{L}^*), && (3.28)
\end{aligned}$$

because in general,

$$\begin{aligned}
\text{if} \quad & \mathcal{L} = \mathcal{L}(\mathbb{B}), \quad \mathbb{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n), && (3.29)\\
\text{then} \quad & \mathcal{L}^* = \mathcal{L}(\mathbb{D}), \quad \mathbb{D} = (\mathbf{d}_1, \dots, \mathbf{d}_n), && (3.30)
\end{aligned}$$

where $\mathbf{b}_i \cdot \mathbf{d}_j = \delta_{ij}$, i.e.,

$$\mathbb{B}^T\mathbb{D} = I, \qquad (3.31)$$

i.e., $\mathcal{L}^* = \mathcal{L}(\mathbb{B}^{-T}\mathbb{Z}^n)$. Note that $\det L^* = (\det L)^{-1}$. □

Corollary 3.1.2. $\rho_r(L + \mathbf{c}) \in r^n \det L^*(1 \pm \varepsilon)$ if $r \geq \eta_\varepsilon(L)$, i.e., $|\rho_{\frac{1}{r}}(L^* \setminus 0)| \leq \varepsilon$, i.e., $\rho_{\frac{1}{r}}$ is very steep.

Proof.

$$\begin{aligned}
\rho_r(L + \mathbf{c}) &= \sum_{x\in L} \rho_r(\mathbf{x} + \mathbf{c}) && (3.32)\\
&= \sum_{\mathbf{x}\in L} \rho_{r,-\mathbf{c}}(\mathbf{x}) && (3.33)\\
&= \det L^* \sum_{\mathbf{y}\in L^*} \widehat{\rho_{r,-\mathbf{c}}}(\mathbf{y}) && (3.34)\\
&= r^n \det L^* \sum_{\mathbf{y}\in L^*} e^{2\pi i\langle \mathbf{c},\mathbf{y}\rangle}\rho_{\frac{1}{r}}(\mathbf{y}) && (3.35)\\
&= r^n \det L^*(1 \pm \varepsilon). && (3.36)
\end{aligned}$$

□

Smoothing parameter [MR04]

$\eta_\varepsilon(L)$, defined above, is called the smoothing parameter, because if $r \geq \eta_\varepsilon(L)$, then ρ_r is rather flat, smooth, and $\rho_r(L{+}c)$ is almost uniform with respect to c. More quantitatively.

- $\eta_\varepsilon(L) \geq \sqrt{n}/\lambda_1(L^*)$ where $\varepsilon = 2^{-n}$ (Micciancio and Regev [MR04]).

- $\exists \varepsilon \le 2e^{-\pi s^2}$ such that $\rho_s(c+\mathbb{Z}) \in \left[1 \pm \frac{\varepsilon}{1-\varepsilon}\right] s$ for all $c \in \mathbb{R}$. Just we compute (note that $\rho_s(c+\mathbb{Z}) \le \rho_s(\mathbb{Z})$)

$$2\sum_{n=1}^{\infty} e^{-\pi(sn)^2} < \frac{2e^{-\pi s^2}}{1-e^{-\pi s^2}} < \frac{\varepsilon}{1-\varepsilon} \tag{3.37}$$

  for some $\varepsilon < 2e^{-\pi s^2}$. (True if ε is sufficiently close to $2e^{-\pi s^2}$.)

- The above example can be generalized to lattice $\mathcal{L} \subset \mathbb{Z}^n \subset \mathbb{R}^n$.
  $\exists \varepsilon < 2ne^{-\pi(\frac{s}{M})^2}$ such that $\rho_s(\mathbf{c}+\mathcal{L}) \in [1 \pm \varepsilon] s^n$ for all $\mathbf{c} \in \mathbb{R}^n$, where $M = \max_i \|\widetilde{b_i}\|$.
  Especially if $s > \sqrt{\log n} M$, then $\rho_s(\mathbf{c}+\mathcal{L}) \in (1 \pm \varepsilon)\frac{1}{\mathrm{poly}(n)}$.

Remark 3.1.3.

- $\rho_s(\mathbf{x}) = e^{-\frac{\pi\|\mathbf{x}\|^2}{s^2}} = \rho_s(x_1)\cdots\rho_s(x_n)$
- $\rho_s(\mathcal{L}(\mathbb{B})) \le \rho_s(\mathcal{L}(\widetilde{\mathbb{B}})) < \prod_{i=1}^{n}\left(1 + \frac{\varepsilon_i}{1-\varepsilon_i}\right) s^n$ for some $\varepsilon_1, \ldots, \varepsilon_n$, where

$$\varepsilon_i < 2\exp\left(-\pi\left(\frac{s}{\|\widetilde{\mathbb{B}}_i\|}\right)^2\right). \tag{3.38}$$

  $\rho_s(\mathcal{L}(\mathbb{B})) \le \rho_s(\mathcal{L}(\widetilde{\mathbb{B}}))$ follows from

$$\mathbb{B} = Q\begin{pmatrix} \|\widetilde{\mathbf{b}_1}\| & & * \\ & \ddots & \\ 0 & & \|\widetilde{\mathbf{b}_n}\| \end{pmatrix}, \tag{3.39}$$

  where Q is orthogonal.

Discrete Gaussians

Definition 1. Discrete Gaussian distribution over coset $\mathbf{c}+\mathcal{L}$ is defined as

$$D_{\mathbf{c}+\mathcal{L},s}(\mathbf{x}) = \frac{\rho_s(\mathbf{x})}{\rho_s(\mathbf{c}+\mathcal{L})} \tag{3.40}$$

for all $\mathbf{x} \in \mathbf{c}+\mathcal{L}$.

Note that if s is sufficiently large (e.g., $s > \eta_\varepsilon(\mathcal{L})$), then the denominator is very close to $s^n \det \mathcal{L}^*$ (e.g., with $\varepsilon = 2^{-n}$, $s > \sqrt{n}/\lambda_1(\mathcal{L}^*)$), and the numerator is the restriction of $\rho_s(x)$ on $\mathbf{c}+\mathcal{L}$. Hence, we only obtain exponentially small information about $\mathbf{c}+\mathcal{L}$ when sampled from $D_{\mathbf{c}+\mathcal{L},s}$ if $s \sim \sqrt{n}/\lambda_1(\mathcal{L}^*)$.

Choose $\mathbf{x} \in \mathbb{Z}^n$ from $D_{\mathbb{Z}^n,s}$, where $s > \eta_\varepsilon(\mathcal{L})$. Reveal the coset $\mathbf{x}+\mathcal{L}$. Then every coset $\mathbf{c}+\mathcal{L}$ is almost equally likely, i.e., the distribution is almost uniform over $\mathbb{Z}^n/\mathcal{L}$. Given $\mathbf{x} \in \mathbf{c}+\mathcal{L}$, it has the conditional distribution $D_{\mathbf{c}+\mathcal{L},s}$.

Let

$$A \leftarrow \mathbb{Z}_q^{n\times m}, \text{ i.e., uniformly} \tag{3.41}$$

$$\mathbf{x} \leftarrow D_{\mathbb{Z}^m,s} \tag{3.42}$$

define $f_A(\mathbf{x}) := A\mathbf{x}(=\mathbf{u}) \in \mathbb{Z}_q^n$. Then, inverting $f_A \Leftrightarrow$ decoding uniform syndrome $\mathbf{u} \Leftrightarrow$ solving SIS for A. (Solving $A\mathbf{x} = \mathbf{u}$ is equivalent to solving $[A|\mathbf{u}]\left[\begin{smallmatrix}\mathbf{x}\\-1\end{smallmatrix}\right] = 0$.)

Conditional distribution when $A\mathbf{x} = \mathbf{u}$ is $D_{\mathcal{L}_{\mathbf{u}}^{\perp}(A),s}$, where

$$\mathcal{L}_{\mathbf{u}}^{\perp} = \{\mathbf{x} \in \mathbb{Z}^n | A\mathbf{x} = \mathbf{u} \mod q\}.$$

3.1.2 Sampling

Algorithms of Gaussian Sampling of $D_{\mathcal{L}_{\mathbf{u}}^{\perp}(A),s}$

(As remarked before, $D_{\mathcal{L}_{\mathbf{u}}^{\perp}(A),s}$ sample does not reveal syndrome $\mathbf{u}$ if

$$\sqrt{\log m} \max \|\widetilde{\mathbf{b}_i}\| \leq s,$$

where $S = (\mathbf{b}_1, \dots, \mathbf{b}_m)$ is a short enough basis of $\mathcal{L}^{\perp}(A)$, since $\varepsilon_i = \frac{1}{\mathcal{O}(\text{poly}(m))}$ in this case.)

Nearest plane algorithm with randomized rounding

Gaussian sample a hyperplane in the coset $\mathcal{L}_{\mathbf{u}}^{\perp}(A)$ which is parallel to $\text{span}\{\mathbf{s}_1, \dots, \mathbf{s}_{m-1}\}$, where $S = \{\mathbf{s}_1, \dots, \mathbf{s}_m\}$ is a basis of $\mathcal{L}^{\perp}(A)$. Then consider the $\mathbb{Z}$ span of $\mathbf{s}_1, \dots, \mathbf{s}_{m-1}$ displaced by the closest vector from the origin to the chosen hyperplane. Do Gaussian sampling on this displaced $(m-1)$-dimensional lattice. Iterate this process. Note that $\rho_s((\mathbf{c} + \mathcal{L}) \bigcap \text{plane})$ depends only on $\text{dist}(0, \text{plane})$, since $\rho_s(\mathbf{x})$ depends only on $\|\mathbf{x}\|$.

Remark 3.1.4. Gaussian nearest plane algorithm for sampling $D_{\mathcal{L}_{\mathbf{u}}^{\perp}(A),s}$ is not efficient and inherently sequential. We need a more efficient Gaussian sampling.

Randomized Babai's roundoff algorithm. [Bab85]

Babai's roundoff algorithm for finding the representative of a coset in the fundamental parallelepiped can be written as

$$\mathbf{c} \mapsto S frac(S^{-1}\mathbf{c}), \tag{3.43}$$

where $S = \{\mathbf{s}_1, \dots, \mathbf{s}_m\}$ is a basis of $\mathcal{L}^{\perp}(A)$.

Naive randomized rounding: Note that $frac(S^{-1}\mathbf{c}) \in \left[-\frac{1}{2}, \frac{1}{2}\right)^m \subset \mathbb{R}^m$. Gaussian sample from $frac(S^{-1}\mathbf{c}) + \mathbb{Z}^m$, i.e., instead of the deterministic $frac(S^{-1}\mathbf{c})$, we could get $frac(S^{-1}\mathbf{c}) + \vec{\mathbf{p}}$ for some $\vec{\mathbf{p}} \in \mathbb{Z}^m$. Then apply S to obtain $\mathbf{x}$. But then we have nonspherical Gaussian distribution of $\mathbf{x}$, because even though $frac(S^{-1}\mathbf{c}) + \vec{\mathbf{p}}$ is spherical Gaussian, when we apply S to $frac(S^{-1}\mathbf{c}) + \vec{\mathbf{p}}$ to obtain $\mathbf{x}$, we have nonspherical discrete Gaussian such that

$$\mathbb{E}_{\mathbf{x}}(\mathbf{x}\mathbf{x}^t) \approx S \cdot S^t, \tag{3.44}$$

where $S = (\mathbf{s}_1, \dots, \mathbf{s}_m)$ is a short basis of $\mathcal{L}^{\perp}(A)$, i.e., it leaks some information about short basis S.

Breakthrough: Gaussian correction

Note that the sum of the Gaussian distribution is again Gaussian with the sum of the covariances as its covariance. (The probability distribution of the sum of two random variables X_1 and X_2 is

$$P_{X_1+X_2}(y) = \int P_{X_1}(x) P_{X_2}(y-x)dx.$$

Hence, $\hat{P}_{X_1+X_2} = \widehat{P}_{X_1}\hat{P}_{X_2}$. In particular, if P_{X_1} and P_{X_2} are Gaussian with covariances s_1^2 and s_2^2, respectively, then $P_{X_1+X_2}$ is Gaussian with covariance $s_1^2+s_2^2$.)

1. Generate perturbation $\mathbf{p}$ with covariance $\sum_2 = \sigma^2 I - \sum_1$, where $\sum_1 = SS^t$, and $\sigma > s_1(S)$, the largest singular value of S.
2. Randomly round off $\mathbf{c}+\mathbf{p}$ to obtain a random sample
$$S \cdot frac(S^{-1}(\mathbf{c}+\mathbf{p})) + \mathcal{L}^{\perp}(A).$$
3. Then add $-\mathbf{p}$.

3.2 Applications

3.2.1 Identity Based Encryption

Identity Based Encryption

- A: $n \times m$ matrix, master public key.
- $\mathbf{u} = H(Alice)$: hashed identity of Alice, public.

Master finds a Gaussian short element in $f_A^{-1}(\mathbf{u})$, i.e., $\mathbf{x} \leftarrow f_A^{-1}(\mathbf{u})$ (Master has a short basis of $\mathcal{L}^{\perp}(A)$), and give Alice $\mathbf{x}$ as her secret key.

I want to send a message bit to Alice so that only Alice can decode. Choose Gaussian short $\mathbf{s}, \mathbf{e} \in \mathbb{Z}_q^n$, $e' \in \mathbb{Z}_q$

$$\mathbf{b}^t := \mathbf{s}^t A + \mathbf{e}^t \tag{3.45}$$
$$b' = \mathbf{s}^t\mathbf{u} + e' + bit \cdot \frac{q}{2} \tag{3.46}$$

Alice decodes: $b' - \mathbf{b}^t\mathbf{x} \approx bit \cdot \frac{q}{2}$.
(Note that this protocol is just a little modification of dual LWE cryptosystem.)

It seems that it is required to have a lattice together with a short basis when we apply SIS or LWE to cryptography. But it is not a simple job to generate a lattice together with a short basis.

The following **signature** protocol is a typical application of a lattice together with a short basis.

- $pk = A$, $sk =$ short basis of $\mathcal{L}^{\perp}(A)$.
- $H : \{0,1\}^* \to \mathbb{Z}_q^n$ random oracle.
- $sign(msg)$: let $\mathbf{u} = H(msg)$, and output Gaussian $\mathbf{x} \leftarrow f_A^{-1}(\mathbf{u})$.
- $verify(msg, \mathbf{x})$: check $f_A(\mathbf{x}) = A\mathbf{x} = H(msg)$ and $\mathbf{x}$ is short enough.

Chapter 4

Constructing Trapdoors and More Applications

4.1 Strong trapdoor generation and inversion algorithms

4.1.1 Methods

Step 1: Gadget G and Inversion Algorithms

Let $q = 2^k$ (It could be generalized to an arbitrary q). Define a $1 \times k$ matrix $g := [1 \quad 2 \quad 4 \quad \cdots 2^{k-1}] \in \mathbb{Z}_q^{1\times k}$. Then the columns of

$$S = \begin{pmatrix} 2 & & & & \\ -1 & 2 & & & \\ & -1 & & & \\ & & \ddots & & \\ & & & 2 & \\ & & & -1 & 2 \end{pmatrix} \tag{4.1}$$

is a lattice basis of $\mathcal{L}^{\perp}(g)$, and $\widetilde{S} = 2I_k$ (Gram-Schmidt orthogonalization).
For q not a power of 2, let $k = \lceil \log(q) \rceil$ so $q < 2^k$. Let $g = [1, 2, \ldots, 2^{k-1}] \in \mathbb{Z}_q^{1\times k}$ as before. Then the columns of

$$S = \begin{pmatrix} 2 & & & & q_0 \\ -1 & 2 & & & q_1 \\ & -1 & & & q_2 \\ & & \ddots & & \vdots \\ & & & 2 & q_{k-2} \\ & & & -1 & q_{k-1} \end{pmatrix} \in \mathbb{Z}^{k\times k} \tag{4.2}$$

is a short basis of $\mathcal{L}^{\perp}(g)$, where $q = \sum_{i=0}^{k-1} 2^i q_i$ is the binary expansion of q. (Note that $\det S = q$.)

- Inversion of LWE with only one equation

$$g_q = sg + e = [s + e_0, 2s + e_1, \ldots, 2^{k-1}s + e_{k-1}] \mod q, \tag{4.3}$$

where $s \in \mathbb{Z}_q$, small $e_i \in \mathbb{Z}$.

Get least significant bit from $2^{k-1}s + e_{k-1}$, i.e., write $s = s_0 + s_1 2 + \cdots + s_{k-1}2^{k-1}$, then

$$2^{k-1}s + e_{k-1} \mod q \quad = 2^{k-1}s_0 + e_{k-1}. \tag{4.4}$$

Hence, $s_0 = 0$ if $2^{k-1}s + e_{k-1}$ is short and $s_0 = 1$ if $2^{k-1}s + e_{k-1}$ is not short. Then consider 2^{nd} to the last, i.e.

$$2^{k-2}s + e_{k-2} = 2^{k-2}(s_0 + 2s_1) + e_{k-1} \mod q. \tag{4.5}$$

We subtract $2^{k-1}s_0$ to obtain $2^{k-1}s_1 + e_{k-2}$. Then we get s_1 in the same way as before. This method works exactly when every $e_i = \left[-\frac{q}{4}, \frac{q}{4}\right)$.

- Inversion of $f_g(x) = \langle g, x\rangle = u$.
  For $i \leftarrow 0, 1, \ldots, k-1$, choose $x_i \leftarrow (2\mathbb{Z} + u)$ by Gaussian sampling. Let $u \leftarrow (u - x_i)/2 \in \mathbb{Z}$. Details are as follows. Note

  $$\langle g, x\rangle = x_0 + 2x_1 + 2^2x_2 + \cdots + 2^{k-1}x_{k-1} = u. \tag{4.6}$$

  Hence, x_0 is even or odd according to u. $x_0 \leftarrow 2\mathbb{Z} + u$, Gaussian sampling from $2\mathbb{Z} + u$. Once we get x_0, $(u - x_0)/2 = x_1 + 2x_2 + \cdots$. The same method works to find $x_1, \cdots$.

Define

$$G = I_n \otimes g = \begin{pmatrix} \cdots g \cdots & & & \\ & \cdots g \cdots & & \\ & & \ddots & \\ & & & \cdots g \cdots \end{pmatrix} \in \mathbb{Z}_q^{n \times nk}, \tag{4.7}$$

where $k = \lceil \log q \rceil$ as before. Now f_G^{-1}, g_G^{-1} reduce to n parallel calls to f_g^{-1}, g_g^{-1}.
Also applies to $\mathbb{H}G$ for any invertible $\mathbb{H} \in \mathbb{Z}_q^{n \times n}$ by considering $f_G^{-1} \circ \mathbb{H}^{-1}$ or $\mathbb{H}^{-1} \circ g_G^{-1}$.

Step 2: Randomize G to obtain uniformly random A

Consider $n \times (\bar{m} + nk)$ matrix $[\bar{A}|G]$ for uniform $\bar{A} \in \mathbb{Z}_q^{n \times \bar{m}}$. Then it is easy to solve SIS and LWE for $[\bar{A}|G]$.

- SIS for $[\bar{A}|G]$ is $f^{-1}_{[\bar{A}|G]}(\mathbf{u}) = \mathbf{x}$, where $(\bar{A}|G)\mathbf{x} = \mathbf{u}$, $X = \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{pmatrix}$, $\mathbf{x}_1 \in \mathbb{Z}^{\bar{m}}$, $\mathbf{x}_2 \in \mathbb{Z}^{nk}$.

  $$\bar{A}\mathbf{x}_1 + G\mathbf{x}_2 = \mathbf{u}. \tag{4.8}$$

  To obtain such $\mathbf{x}$, choose small $\mathbf{x}_1$, then apply f_G^{-1} to $\mathbf{u} - \bar{A}\mathbf{x}_1$ to get $\mathbf{x}_2$.

- LWE for $[\bar{A}|G]$, $\mathbf{s}^t(\bar{A}|G) + \mathbf{e}^t = (\mathbf{s}^t\bar{A} + \mathbf{e}_1^t|\mathbf{s}^tG + \mathbf{e}_2^t) = (\mathbf{b}_1^t|\mathbf{b}_2^t)$. Apply g_G^{-1} to $\mathbf{b}_2^t$ to obtain $\mathbf{s}$, since

  $$\mathbf{s}^tG + \mathbf{e}_2^t = \mathbf{b}_2^t. \tag{4.9}$$

  And confirm $\mathbf{s}$ satisfies $\mathbf{s}^t\bar{A} + \mathbf{e}_1 = \mathbf{b}_1^t$.

To obtain random matrix A, choose short Gaussian $R \leftarrow \mathbb{Z}^{\bar{m}\times n\lceil \log q\rceil}$ and

$$\begin{aligned} A &:= (\bar{A}|G)\begin{pmatrix} I & -R \\ 0 & I \end{pmatrix} && (4.10)\\ &= (\bar{A}|G-\bar{A}R). && (4.11)\end{aligned}$$

A is uniform if $\bar{A}R$ is uniform. If $\bar{m}\approx n\log q$, $\bar{A}R$ is uniform, since $R\to\bar{A}R$ is uniform from $\mathbb{Z}^{\bar{m}\times n\lceil\log q\rceil}\to\mathbb{Z}_q^{n\times n\lceil\log q\rceil}$, and left over hash lemma applies if $2^{\bar{m}}\approx q^n$, i.e., $\bar{m}\approx n\log q$. (Note that $\left(\begin{smallmatrix} I & R \\ 0 & -R\end{smallmatrix}\right)$ is unimodular, hence the above construction is just a base change.)
Now we have constructed uniformly random $A=(\bar{A}|G-\bar{A}R)$.

Definition 2. R is a trapdoor for A with tag $H\in\mathbb{Z}_q^{n\times n}$, which is invertible, if $A\begin{pmatrix} R \\ \hline I\end{pmatrix} = HG$.

Quality of R is

$$s_1(R)=\max_{\|u\|=1}\|Ru\|. \tag{4.12}$$

(maximal singular value)
From random matrix theory, we know

$$s_1(R)\approx(\sqrt{\#rows}+\sqrt{\#colums})r \tag{4.13}$$

for Gaussian entries with standard deviation r.

Remark 4.1.1. Let $S\in\mathbb{Z}^{w\times w}$ be any basis for $\mathcal{L}^{\perp}(G)$. ($w=nk$)
$A\in\mathbb{Z}_q^{n\times m}$ have trapdoor $R\in\mathbb{Z}^{(m-w)\times w}$ with tag $H\in\mathbb{Z}_q^{n\times n}$. Then $\mathcal{L}^{\perp}(A)$ is generated by the basis

$$S_A=\begin{pmatrix} I & R \\ 0 & I\end{pmatrix}\begin{pmatrix} I & 0 \\ W & S\end{pmatrix}, \tag{4.14}$$

where $W\in\mathbb{Z}^{w\times\bar{m}}$ is an arbitrary solution to

$$GW=-H^{-1}A(I|0)^T \mod q. \tag{4.15}$$

Note that both sides are $n\times\bar{m}$ matrices, and $m=\bar{m}+w$. Hence, $(I|0)$ is an $\bar{m}\times m$ matrix. Eq. (4.15) has many solutions since W has $w\times\bar{m}$ unknowns and the right hand side gives $n\times\bar{m}$ conditions and G is a rank n matrix.. It is easy to check $AS_A=0$ mod q, and $\det(S_A)=\det S=q^n=\det(\mathcal{L}^{\perp}(A))$. (We assume $\mathbb{Z}^m\ni\mathbf{x}\to A\mathbf{x}\in\mathbb{Z}_q^n$ is onto.) Let us consider the Gram-Schmidt Orthogonalization of S_A,

$$\widetilde{S}_A=\widetilde{TB}, \tag{4.16}$$

where $B=\begin{pmatrix} I & 0 \\ W & S\end{pmatrix}$ and $T=\begin{pmatrix} I & R \\ 0 & I\end{pmatrix}$. $\widetilde{B}=\begin{pmatrix} I & 0 \\ 0 & \widetilde{S}\end{pmatrix}$, hence $\|\widetilde{B}\|=\|\widetilde{S}\|$.

Now we prove $\|\widetilde{TB}\|\le s_1(T)\|\widetilde{B}\|$.
Let

$$B=QDU,\quad TB=Q'D'U' \tag{4.17}$$

by the Gram-Schmidt decomposition of B and TB, respectively, where Q is orthogonal, D is positive diagonal, and U is upper triangular.

$$TQDU=Q'D'U'\Rightarrow T'D=D'U'', \tag{4.18}$$

where $T' = Q'^{-1}TQ$ and $U'' = U'U^{-1}$. Then

$$\|\widetilde{TB}\| = \|D'\| \le \|D'U''\| = \|T'D\| \le s_1(T')\|\widetilde{B}\| = s_1(T)\|\widetilde{B}\| = s_1(T)\|\widetilde{S}\|, \tag{4.19}$$

since the ith row of $D'U''$ has the norm at least $d'_{i,i}$, the i-th diagonal of D'.
Since

$$T = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} + \begin{pmatrix} 0 & R \\ 0 & 0 \end{pmatrix}$$

and $s_1(T) \le s_1(R) + 1$, it follows that

$$\|\widetilde{S}_A\| \le (s_1(R) + 1)\|\widetilde{S}\|. \tag{4.20}$$

Suppose that $A\binom{R}{I} = G$.

- Given a LWE problem with coefficient matrix A,

$$\mathbf{b}^t = \mathbf{s}^t A + \mathbf{e}^t, \tag{4.21}$$

we can recover $\mathbf{s}$ from the LWE problem with coefficient matrix G,

$$\mathbf{b}^t \left(\frac{R}{I}\right) = \mathbf{s}^t G + \mathbf{e}^t \left(\frac{R}{I}\right). \tag{4.22}$$

It works if each entry of $\mathbf{e}^t\left(\frac{R}{I}\right)$ is in $\left(-\frac{q}{4}, \frac{q}{4}\right)$, i.e., $\|\mathbf{e}\| < \frac{q}{4s_1\left(\frac{R}{I}\right)}$.

- Sampling Gaussian preimage.
Given $\mathbf{u}$, sample $\mathbf{z} \leftarrow f_G^{-1}(\mathbf{u})$ and output $\mathbf{x} = \left(\frac{R}{I}\right)\mathbf{z} \in f_A^{-1}(\mathbf{u})$.
Then we have $A\mathbf{x} = G\mathbf{z} = \mathbf{u}$ as desired, i.e., we obtained an SIS solution $\mathbf{x}$ with respect A from an SIS solution with respect to G.

  But there is the problem as before that $\left(\frac{R}{I}\right)\mathbf{z}$ is nonspherical even though $\mathbf{z}$ is spherical, i.e., it leaks R. This can be cured as before. The covariance of $\mathbf{x} = \left(\frac{R}{I}\right)\mathbf{z}$ is

$$\sum = \mathbb{E}_{\mathbf{x}}(\mathbf{x}\cdot\mathbf{x}^t) = \mathbb{E}_{\mathbf{z}}\left(\left(\frac{R}{I}\right)\mathbf{z}\cdot\mathbf{z}^t\left(\frac{R}{I}\right)^t\right) \approx s^2RR^t, \tag{4.23}$$

when $\mathbf{z}$ spherical Gaussian with deviation s.

  Choose $s > s_1(R)$ and let $\sum_2 = s^2I - RR^t > 0$.
Generate perturbation $\mathbf{p}$ with covariance $\sum_2$. Sample a spherical $\mathbf{z}$ such that $G\mathbf{z} = \mathbf{u} - A\mathbf{p}$. Output $\mathbf{x} = \mathbf{p} + \left(\frac{R}{I}\right)\mathbf{z}$. This algorithm generates a spherical discrete Gaussian over $\mathcal{L}_{\mathbf{u}}^{\perp}(A)$.

4.2 Applications

Efficient IBE

1. Choose $A = (\bar{A}| - \bar{A}R)$. Let $mpk = (A, u)$, $msk = R$ (A has trapdoor R with tag 0).

2. map: id $\rightarrow$ invertible $H_{id} \in \mathbb{Z}_q^{n\times n}$
choose $sk_{id} : x \leftarrow f_{A_{id}}^{-1}(u)$ using the above algorithm, sampling Gaussian preimage, where $A_{id} = A + (0|H_{id}G) = (\bar{A}|H_{id}G - \bar{A}R)$.

3. Encrypt to A_{id}, decrypt using sk_{id} as in dual public key cryptosystem.

Part II

Introduction to Ring-LWE

Chapter 5

Preliminaries for Ring-LWE cryptography

5.1 Notations

In Part II, we use the notations in [LPR13].

- $\forall \bar{a} \in \mathbb{R}/\mathbb{Z}$, $[\![\bar{a}]\!] \in \mathbb{R}$ denotes the unique representative, where $a \in (\bar{a}+\mathbb{Z}) \bigcap \left[-\frac{1}{2}, \frac{1}{2}\right)$.

- $\forall \bar{a} \in \mathbb{Z}_q$, $[\![\bar{a}]\!]$ denotes the unique representative $a \in (\bar{a} + q\mathbb{Z}) \bigcap [-q/2, q/2)$.

- $[k] = \{0, 1, \ldots, k-1\}$.

- $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$.

- $\mathbb{Z}_m^* \subset \mathbb{Z}_m$: the set of invertible elements mod m.

- $|\mathbb{Z}_m^*| = \varphi(m)$: Euler totient.

- $H = \{x \in \mathbb{C}^{\mathbb{Z}_m^*} : x_i = \overline{x_{m-i}}, \forall i \in \mathbb{Z}_m^*\}$. Note that if $(i, m) = 1$ (relatively prime), then $(m-i, m) = 1$ also.

- $H \cong \mathbb{R}^{[n]}$, $n = \varphi(m)$.

- $B = \frac{1}{\sqrt{2}} \begin{pmatrix} I & \sqrt{-1}J \\ J & -\sqrt{-1}I \end{pmatrix}$ unitary basis of H, where

$$I = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}, \qquad J = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & \iddots & & \\ 1 & & & \end{pmatrix},$$

  $\frac{1}{\sqrt{2}}(e_i + e_{m-i})$ for $i < m/2$ and $i \in \mathbb{Z}_m^*$, $\frac{\sqrt{-1}}{\sqrt{2}}(e_i - e_{m-i})$ for $i > \frac{m}{2}$ and $i \in \mathbb{Z}_m^*$. We read B as a $\mathbb{Z}_m^*$-by-$[n]$ matrix.

5.2 Gaussians and Subgaussian Random Variables

We follow [LPR13] as before, giving some details.

Definition 3. Random variable X over $\mathbb{R}$ is δ-subgaussian with parameter $s > 0$ if for all $t \in \mathbb{R}$

$$\mathbb{E}[\exp(2\pi t X)] \leq \exp(\delta) \cdot \exp(\pi s^2 t^2). \tag{5.1}$$

Lemma 5.2.1. *$Pr(|X| \geq \alpha) \leq 2\exp(\delta - \pi\alpha^2/s^2)$.*

Proof. From the definition, Markov inequality[1] says

$$Pr(X > \alpha) \leq \exp(\delta) \cdot \exp(\pi s^2 t^2 - 2\pi t\alpha) \tag{5.2}$$

for any t. RHS becomes minimum at $t = \frac{\alpha}{s^2}$, and its value is $\exp(\delta) \cdot \exp\left(-\frac{\pi\alpha^2}{s^2}\right)$. Similarly, $Pr(X < -\alpha) \leq \exp(\delta) \cdot \exp(\pi s^2 t^2 - 2\pi t\alpha)$. □

Example 5.2.1. If $\mathbb{E}(X) = 0$ and $|X| \leq B$, then X is 0-subgaussian with parameter $B\sqrt{2\pi}$.

Proof. Let $p(x)$ be a probability distribution of random variable X. Then

$$\mathbb{E}(\exp(2\pi t X)) = \int_{-B}^{B} e^{2\pi t x} p(x)dx, \tag{5.3}$$

where $\mathbb{E}(x) = \int_{-B}^{B} xp(x)dx = 0$ and $\int_{-B}^{B} p(x) = 1$. Simplex method says that the maximum of $\int_{-B}^{B} \exp(2\pi t x)p(x)dx$ occurs when $p(x)$ is a boundary point of the simplex of the probability space satisfying the given conditions, i.e., $p(x) = (\delta_B(x) + \delta_{-B}(x))/2$, and its value is $\frac{e^{2\pi tB} + e^{-2\pi tB}}{2} = \cosh(2\pi tB) \leq \exp(2\pi^2 B^2 t^2)$. Hence, X is 0-subgaussian with parameter $B\sqrt{2\pi}$. □

Remark 5.2.2. We can prove $e^x + e^{-x} \leq 2e^{x^2/2}$ by series expansion.

Lemma 5.2.3. *If the conditional probability $Pr(X_i|X_1, \ldots, X_{i-1})$ is δ_i-subgaussian with parameter s_i for $i = 1, \ldots, k$, then $\sum X_i$ is $(\sum \delta_i)$-subgaussian with parameter $(\sum s_i^2)^{1/2}$.*

Proof. We may assume $k = 2$.

$$\begin{aligned} \mathbb{E}(\exp 2\pi t(X_1 + X_2)) &= \mathbb{E}_{X_1}\left(\exp(2\pi t X_1)\mathbb{E}_{X_2}(\exp 2\pi t X_2|X_1)\right) & (5.4)\\ &\leq \exp(\delta_1 + \delta_2)\exp(\pi(s_1^2 + s_2^2)t^2). & (5.5) \end{aligned}$$

□

Lemma 5.2.4. *Let X be δ-subgaussian with parameter s. Then for any $t \in \left(0, \frac{1}{2s^2}\right)$,*

$$\mathbb{E}(\exp(2\pi t X^2)) \leq 1 + 2\exp(\delta) \cdot \left(\frac{1}{2ts^2} - 1\right)^{-1}. \tag{5.6}$$

[1] For any positive and increasing function f, $\mathbb{E}(f(X)) = \int_{-\infty}^{\infty} f(x)p(x)dx \geq \int_{\alpha}^{\infty} f(x)p(x)dx \geq f(\alpha)Pr(X > \alpha)$, so $Pr(X > \alpha) \leq \mathbb{E}(f(X))/f(\alpha)$.

Proof. By Lemma 5.2.1,

$$\exp(2\pi tr^2)Pr(|X| > r) \leq 2\exp(\delta)\exp(\pi(2t - 1/s^2)r^2), \tag{5.7}$$

and since $t < 1/2s^2$ by assumption, $2t - 1/s^2 < 0$, so

$$\lim_{r\to\infty} \exp(2\pi tr^2)Pr(|X| > r) = 0. \tag{5.8}$$

Now let $Pr(|X| > r) = f(r)$. Then

$$df = -(p(x) + p(-x))dx, \tag{5.9}$$

where $p(x)$ is the probability density, since $f(r) = \int_r^\infty p(x)dx + \int_{-\infty}^{-r} p(x)dx$. Hence,

$$\begin{aligned}
\mathbb{E}(\exp(2\pi tX^2)) &= \int_0^\infty e^{2\pi tr^2}(p(r) + p(-r))dr && (5.10)\\
&= -\int_0^\infty e^{2\pi tr^2} d(Pr(|X| \geq r)) && (5.11)\\
&= 1 + \int_0^\infty d(e^{2\pi tr^2})Pr(|X| \geq r) && (5.12)\\
&\quad \text{(Since } e^{2\pi tr^2}Pr(|X| > r) = 1 \text{ when } r = 0\text{, and by (5.8).)}\\
&= 1 + \int_0^\infty Pr(|X| > r)4\pi tr\exp(2\pi tr^2)dr && (5.13)\\
&\leq 1 + 8\pi t\exp(\delta)\int_0^\infty r\exp(-\pi r^2/s^2 + 2\pi tr^2)dr && (5.14)\\
&\quad \text{(Since } t > 0 \text{ and by (5.7).)}\\
&= 1 + 2\exp(\delta)\left(\frac{1}{2ts^2} - 1\right)^{-1} && (5.15)\\
&\leq \exp\left(2\exp(\delta)\left(\frac{1}{2ts^2} - 1\right)^{-1}\right). && (5.16)
\end{aligned}$$

□

Lemma 5.2.5. If $X_1, \ldots, X_k$ are random variables each of which is δ-subgaussian with parameter s conditioned on any values of the previous ones, then for any $r > k's^2/\pi$ where $k' = 2k\exp(\delta)$, we have that

$$Pr\left(\sum X_i^2 > r\right) \leq \exp\left(k'\left(2\left(\frac{\pi r}{k's^2}\right)^{1/2} - \frac{\pi r}{k's^2} - 1\right)\right). \tag{5.17}$$

Proof. From the previous lemma,

$$\mathbb{E}\left(\exp\left(2\pi t\sum X_i^2\right)\right) \leq \exp\left(2k\exp(\delta)\left(\frac{1}{2ts^2} - 1\right)^{-1}\right), \tag{5.18}$$

where $0 < t < 1/2s^2$. Hence,

$$Pr\left(\sum X_i^2 > r\right) \leq \exp\left(2k\exp(\delta)\left(\frac{1}{2ts^2} - 1\right)^{-1} - 2\pi tr\right). \tag{5.19}$$

Letting $x = 2s^2t$ and $A = \pi r/(s^2k')$ (note that $0 < x < 1$ and $A > 1$ by assumption), the expression inside the exponent can be written as

$$2k\exp(\delta)\left(\left(\frac{1}{x}-1\right)^{-1} - Ax\right). \tag{5.20}$$

The minimum of $(\frac{1}{x}-1)^{-1} - Ax$ is $2\sqrt{A} - A - 1$, obtained at $x = 1 - \frac{1}{\sqrt{A}}$. □

Remark 5.2.6. Since $2\alpha^{1/2} - \alpha - 1 < -\alpha/4$ for all $\alpha \geq 4$,

$$Pr(\sum X_i^2 > r) \leq \exp\left(-\frac{\pi r}{4s^2}\right) \tag{5.21}$$

for any $r \geq 4k's^2/\pi$.

Definition 4. An $\mathbb{R}^n$-valued random variable X is δ-subgaussian with parameter s if for all unit vectors $\mathbf{u} \in \mathbb{R}^n$, $\langle X, \mathbf{u}\rangle$ is δ-subgaussian with parameter s.

Note that if the coordinates of X are independent and all are δ-subgaussian with parameter s, then X is $n\delta$-subgaussian with the same parameter s. (If $u = (u_1, \dots, u_n)$ and $u_1^2 + \dots + u_n^2 = 1$, then u_iX_i is δ-subgaussian with parameter $|u_i|s$.)

Corollary 5.2.7. For $i = 1, \dots, k$, let X_i be random vectors in $\mathbb{R}^n$, and A_i $n \times n$ matrices. For δ_i, $s_i \geq 0$, suppose that X_i is δ_i-subgaussian with parameter s_i conditioned on any values of $X_1, \dots, X_{i-1}$. Then $\sum A_iX_i$ is $(\sum \delta_i)$-subgaussian with parameter $\lambda_{\max}(\sum s_i^2 A_i A_i^T)^{1/2}$.

Proof. For any unit vector $\mathbf{u} \in R^n$,

$$\left\langle \sum_i A_iX_i, \mathbf{u} \right\rangle = \sum_i \langle A_iX_i, \mathbf{u}\rangle = \sum_i \left\langle X_i, A_i^T\mathbf{u}\right\rangle. \tag{5.22}$$

Note that $\left\langle X_i, A_i^T\mathbf{u}\right\rangle$ is δ_i-subgaussian with parameter $s_i\|A_i^T\mathbf{u}\|_2$ conditioned on any value of the previous ones. Hence, the sum is $(\sum \delta_i)$-subgaussian with parameter

$$\left(\sum s_i^2\|A_i^T\mathbf{u}\|_2^2\right)^{1/2} = ((\mathbf{u}^T\sum s_i^2A_iA_i^T)\mathbf{u})^{1/2}, \tag{5.23}$$

whose maximum over all unit vectors $\mathbf{u}$ is $\lambda_{\max}(\sum s_i^2A_iA_i^T)^{1/2}$. □

5.3 Lattice Background

Let $\Lambda = \mathcal{L}(B) = \{\sum_j z_j\mathbf{b}_j : z_j \in \mathbb{Z}\}$ be a lattice in H generated by a basis $B = \{\mathbf{b}_j\} \subset H$. We define dual lattice of $\Lambda \subset H$ as $\Lambda^\vee = \{y \in H : \forall x \in \Lambda, \langle x, \bar{y}\rangle = \sum x_iy_i \in \mathbb{Z}\}$. Note that this is actually the complex conjugates of the dual lattice as usually defined in $\mathbb{C}^n$. If $\Lambda = \mathcal{L}(B)$, where $B = \{\mathbf{b}_j\} \subset H$, the dual basis $D = \{\mathbf{d}_j\}$ is characterized by $\left\langle \mathbf{b}_i, \bar{\mathbf{d}}_k\right\rangle = \delta_{jk}$, i.e., $BD^T = I$, i.e., $D = B^{T-1}$.

Remark 5.3.1.

1. $\frac{\rho_s}{s^n}$ is a probability distribution on $\mathbb{R}^n$. Hence, $\frac{\rho_s|_\Lambda}{s^n}\det\Lambda$ is almost a probability distribution on the lattice Λ. In particular, $\frac{\rho_s(\Lambda)}{s^n}\det\Lambda \approx 1$. More precisely, if $s \geq \eta_\varepsilon(\Lambda)$, where $\eta_\varepsilon(\Lambda)$ is the smoothing parameter defined earlier, then $\rho_s(\Lambda+c) \in (1+\varepsilon)s^n \det(\Lambda)^{-1}$ ([Reg05]).

2. For any n-dimensional lattice Λ and $s > 0$, a point sampled from $D_{\Lambda,s} = \frac{\rho_s}{\rho_s(\Lambda)}$ has the Euclidean norm of at most $s\sqrt{n}$ except with probability at most 2^{-2n} ([Ban93]).

3. There is an efficient algorithm that samples to within $negl(n)$ statistical distance of $D_{\Lambda+c,s}$ given $c \in H$, a basis B of Λ, and a parameter $s \geq \max_j \|\tilde{b_j}\|\omega(\sqrt{\log n})$ ([GPV08]), where we define the discrete Gaussian probability distribution over $\Lambda + c$ as

$$D_{\Lambda+c,s(x)} = \frac{\rho_s(x)}{\rho(\Lambda+c)}, \forall x \in \Lambda + c. \tag{5.24}$$

Note c is not the center of $D_{\Lambda+c,s}$, since we did not translate D_Λ by c. In comparison, $c + D_\Lambda$ is a c-centered distribution. Rather, we restricted ρ_s on $\Lambda + c$. So the maximum probability of $D_{\Lambda+c,s}$ occurs at the nearest point to the origin.

5.3.1 Decoding

$\Lambda \subset H$: a fixed lattice.
$\mathbf{x} \in H$: an unknown short vector.
We are given $\mathbf{t}$ such that $\mathbf{t} = \mathbf{x} \mod \Lambda$. The goal is to recover $\mathbf{x}$.

First attempt

A basis $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ is known, $\mathbf{t} = \sum c_i\mathbf{b}_i$, and claim $\mathbf{x} = \sum(c_i - \lceil c_i \rfloor)\mathbf{b}_i$, i.e., Babai's round off algorithm with respect to the basis B [Bab85].

Problem: If the basis B are not short, then $\sum(c_i - \lceil c_i \rfloor)\mathbf{b}_i$ not short in general. Hence, in that case it couldn't be $\mathbf{x}$, because $\mathbf{x}$ is rather short. This algorithm succeeds when $|\mathbf{x}| \leq d$, where the ball of radius d is in $P(\mathbb{B})$.

Second attempt

Choose $\{\mathbf{v}_i\}$, a fixed set of n linearly independent and typically short vectors in the dual lattice $\Lambda^\vee$ ($\{\mathbf{v}_i\}$ need not be a basis of $\Lambda^\vee$). Denote the dual basis of $\{\mathbf{v}_i\}$ by $\{\mathbf{b}'_i\}$, and let $\Lambda' \supset \Lambda$ be the super lattice generated by $\{\mathbf{b}'_i\}$. Given an input $\mathbf{t} = \mathbf{x} \mod \Lambda$, we re-express $\mathbf{t}$ in $\bmod \Lambda'$ with respect to the basis $\{\mathbf{b}'_i\}$ as $\sum c_i\mathbf{b}'_i$, $c_i \in \mathbb{R}/\mathbb{Z}$, and output $\sum_i [\![c_i]\!]\mathbf{b}'_i \in H$ (Note that $c_i = \langle \mathbf{x}, \bar{\mathbf{v}}_i\rangle \mod 1$). Hence, the output is equal to $\mathbf{x}$ if and only if all the coefficients $a_i = \langle \mathbf{x}, \bar{\mathbf{v}}_i\rangle$ in the expansion $\mathbf{x} = \sum a_i\mathbf{b}'_i$ are in $[-\frac{1}{2}, \frac{1}{2})$. (Note that in general, $\mathbf{b}'_i \in \Lambda'$ is small but not necessarily in Λ.) Hence, the second attempt works when $\mathbf{x} \in P(B')$. In general, the radius of the ball enclosed in $P(B')$ is larger than the radius of the ball enclosed in $P(B)$ with the given basis $B = (\mathbf{b}_1, \cdots, \mathbf{b}_n)$ even though $\Lambda' \supset \Lambda$, because of the choice of $\{\mathbf{v}_i\}$.

Example 5.3.1. Define a lattice by

$$\mathbf{x} = (x_1, \dots, x_n) \in \Lambda \subset \mathbb{Z}^n \quad \text{if} \quad \sum_i x_i = 0 \mod 2.$$

Then

$$\Lambda^\vee = \mathbb{Z}^n \cup (\mathbb{Z}^n + \frac{1}{2}(1, 1, \ldots, 1)).$$

A basis of Λ is

$$\{(1, 1, 0, \ldots, 0), (1, 0, 1, 0, \ldots), (1, 0, \ldots, 0, 1), (2, 0, \ldots, 0)\},$$

and a basis of $\Lambda^\vee$ is

$$\{(1, 0, \ldots, 0), \cdots, (0, \ldots, 0, 1, 0), \tfrac{1}{2}(1, \ldots, 1)\}.$$

Since

$$\{\mathbf{v}_i\} = \{(1, 0, \ldots, 0), \cdots, (0, \ldots, 0, 1, 0), (0, \ldots, 0, 1)\},$$

$\Lambda^\vee \supset \mathcal{L}(\{\mathbf{v}_i\})$. But $\|\mathbf{v}_i\| = 1$ for $i = 1, \ldots, n$, and $\Lambda' = \mathcal{L}(\{\mathbf{v}_i\})^\vee = \mathbb{Z}^n \supset \Lambda$.

Discretization

Input $\Lambda = \mathcal{L}(B)$ with a good basis $B = \{\mathbf{b}_i\}$, $\mathbf{x} \in H$, $\mathbf{c} \in H$.
The goal is to discretize $\mathbf{x}$ to a point $\mathbf{y} \in \Lambda + \mathbf{c}$ written $\mathbf{y} \leftarrow \lfloor \mathbf{x} \rceil_{\Lambda+\mathbf{c}}$, so that $\mathbf{y} - \mathbf{x}$ is not too large. Hence, it suffices to find a relatively short offset vector $\mathbf{f}$ from the coset $\Lambda + \mathbf{c}' = \Lambda + (\mathbf{c} - \mathbf{x})$ and output $\mathbf{y} = \mathbf{x} + \mathbf{f}$. Note that $\lfloor \mathbf{z} + \mathbf{x} \rceil_{\Lambda+\mathbf{c}}$ and $\mathbf{z} + \lfloor \mathbf{x} \rceil_{\Lambda+\mathbf{c}}$ are identically distributed for any $\mathbf{z} \in \Lambda$ if our algorithm depends only on the coset $\Lambda + \mathbf{c}'$, and not on the particular representative. In this case, it is called valid discretization.

Coordinate-wise randomized rounding:

Given a coset $\Lambda + \mathbf{c}'$, represent $\mathbf{c}' = \sum a_i \mathbf{b}_i \mod \Lambda$ for some coefficient $a_i \in [0, 1)$, then randomly and independently choose f_i from $\{a_i - 1, a_i\}$ to have zero expectation, and output $\mathbf{f} = \sum f_i \mathbf{b}_i \in \Lambda + c'$. Note that f_i is 0-subgaussian with parameter $\sqrt{2\pi}$, hence $\mathbf{f}$ is 0-subgaussian with parameter $\sqrt{2\pi}s_1(B)$, since $|f_i| \leq 1$ and

$$B \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix} = \mathbf{f},$$

where $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$. More directly, let $\mathbf{u}$ be a unit vector. $\langle \mathbf{f}, \mathbf{u} \rangle = \sum f_i \langle \mathbf{b}_i, \mathbf{u} \rangle$, and $f_i \langle \mathbf{b}_i, \mathbf{u} \rangle$ is 0-subgaussian with parameter $\sqrt{2\pi} \cdot |\langle \mathbf{b}_i, \mathbf{u} \rangle|$. Hence, $\langle \mathbf{f}, \mathbf{u} \rangle$ is 0-subgaussian with parameter $(\sum 2\pi |\langle \mathbf{b}_i, \mathbf{u} \rangle|^2)^{1/2} \leq \sqrt{2\pi}s_1(B)$.

5.4 Algebraic Number Theory Background

For a positive integer m, the mth cyclotomic number field is a field extension $K = \mathbb{Q}(\zeta_m)$ obtained by adjoining an element ζ_m of order m (primitive mth root of unity) to the rationals. (Hence, $\mathbb{Q}(\zeta_m) = \mathbb{Q}[\zeta_m]$.) The minimal polynomial of ζ_m is the mth cyclotomic polynomial

$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega_m^i) \in \mathbb{Z}[X], \tag{5.25}$$

where $\omega_m = \mathbf{e}^{2\pi i/m}$.

Since $n = |\mathbb{Z}_m^*| = \varphi(m) :=$ degree of Φ_m, we can view K as a vector space of dimension n over $\mathbb{Q}$, which has a basis $(\zeta_m^j)_{j \in [n]} = (1, \zeta_m, \ldots, \zeta_m^{n-1})$, called the power basis.

Remark 5.4.1. $X^m - 1 = \prod_{d|m} \Phi_d(X)$, where d runs over all the positive divisors of m, because an mth root of unity is a primitive dth root of unity for some divisor d of m, and conversely a primitive dth root of unity is an mth root of unity if d divides m. (Another remark: Decompose $\{0, 1, 2, \ldots, , m-1\}$ according to $\gcd(j, m)$.) In particular,

$$\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$$

for any prime p, and by induction,

$$\Phi_{p^r}(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = \frac{t^p - 1}{t - 1} = 1 + t + \cdots + t^{p-1}, \tag{5.26}$$

where $t = X^{p^{r-1}}$. In general, for any m,

$$\Phi_m(X) = \Phi_{\mathrm{rad}(m)}(X^{m/\mathrm{rad}(m)}),$$

where $\mathrm{rad}(m)$ is the product of all distinct primes dividing m. If m' divides m, we can view $K' = \mathbb{Q}(\zeta_{m'})$ as a subfield of $K = \mathbb{Q}(\zeta_m)$ by identifying $\zeta_{m'}$ with $\zeta_m^{m/m'}$. In general $\Phi_{pq}(X)$ is not of simple form for distinct primes p and q, even though

$$\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1).$$

5.4.1 A key fact from algebraic number theory

Let $m = \Pi_l m_l$ be a prime power factorization i.e., m_l are powers of distinct primes. Then

$$\mathbb{Q}(\zeta_m) \cong \otimes K_l,$$

where $K_l = \mathbb{Q}(\zeta_{m_l})$, via the correspondence $\bigotimes_l a_l \leftrightarrow \prod_l a_l$, where on the right we embed each $a_l \in K_l$ into K as a subfield.

5.4.2 Canonical Embedding and Geometry

Let $K = \mathbb{Q}(\zeta_m)$, and $\omega_m \in \mathbb{C}$ a fixed primitive mth root of unity, for example $e^{2\pi i/m}$. For each $i \in \mathbb{Z}_m^*$, let

$$\sigma_i : K \to \mathbb{C}, \qquad \zeta_m \mapsto \omega_m^i.$$

Clearly $\sigma_i = \bar{\sigma}_{m-i}$, $\forall i \in \mathbb{Z}_m^*$, because $\sigma_i \sigma_{m-i} = 1$, i.e., $\sigma_i = (\sigma_{m-i})^{-1} = \bar{\sigma}_{m-i}$. We define the canonical embedding

$$\sigma : K \to \mathbb{C}^{\mathbb{Z}_m^*}, \qquad a \mapsto \sigma(a) = (\sigma_i(a))_{i \in \mathbb{Z}_m^*}.$$

Hence, $\sigma(K) \subset H \subset \mathbb{C}^{\mathbb{Z}_m^*}$, where H is defined as before. Note that σ is a ring homomorphism from K to H, where multiplication and addition in H are both componentwise.

For $a \in K$, define $\|a\|_2 = \|\sigma(a)\|_2$ and $\|a\|_\infty = \max_i |\sigma_i(a)|$. Then $\|\zeta\|_2 = \sqrt{n}$ and $\|\zeta\|_\infty = 1$.

The map

$$\mathrm{Tr} : K \to \mathbb{Q}, \qquad a \mapsto \sum_{i \in \mathbb{Z}_m^*} \sigma_i(a)$$

is called the trace. Note that

$$\mathrm{Tr}(a \cdot b) = \sum_i \sigma_i(a)\sigma_i(b) = \left\langle \sigma(a), \overline{\sigma(b)} \right\rangle. \tag{5.27}$$

The map

$$N : K \to \mathbb{Q}, \qquad a \mapsto \prod_{i \in \mathbb{Z}_m^*} \sigma_i(a)$$

is called the norm.

Note that $\mathrm{Tr}(a)$ and $\mathrm{N}(a)$ can also be thought of as the trace and the determinant of the multiplication map $\sigma(a) : \mathbb{C}^{\mathbb{Z}_m^*} \to \mathbb{C}^{\mathbb{Z}_m^*}$.

It is trivial to see that

$$\mathrm{N}(ab) = N(a)N(b). \tag{5.28}$$

With the canonical isomorphism $K \cong \bigotimes_l K_l$, we have

$$\sigma\left(\otimes_l a_l\right) = \otimes_l \sigma^{(l)}(a_l), \tag{5.29}$$

$$\mathrm{Tr}_{K/\mathbb{Q}}\left(\otimes_l a_l\right) = \prod_l \mathrm{Tr}_{K_l/\mathbb{Q}}(a_l), \tag{5.30}$$

$$\mathrm{N}(a_1 \otimes \cdots \otimes a_k) = \prod_l \mathrm{N}(a_l)^{m/m_l}. \tag{5.31}$$

5.4.3 The Ring of Integers and Its Ideals

Let $R \subset K$ denote the set of all algebraic integers in a number field K, i.e., $a \in R \subset K$ if and only if it satisfies a monic integral polynomial. R is called the ring of integers. Note that $\mathrm{Tr}, \mathrm{N} : R \to \mathbb{Z}$, and for cyclotomic number field $K = \mathbb{Q}(\zeta_m)$, $R = \mathbb{Z}[\zeta_m] \cong \frac{\mathbb{Z}[x]}{\Phi_m(x)}$. Hence, the power basis $\{\zeta_m^j\}_{j \in [n]}$ is also a $\mathbb{Z}$-basis of R. We can view $R \cong \bigotimes_l R_l$ as before.

Definition 5. Discriminant Δ_K of K is $\Delta_K = \det(\sigma(R))^2$.

$$\Delta_K = \left(\frac{m}{\prod_{\mathrm{prime} p | m} p^{\frac{1}{p-1}}} \right)^n \le n^n, \tag{5.32}$$

for the mth cyclotomic number field and $n = \varphi(m)$. $\Delta_K \le n^n$ follows from $\sigma(R) = \mathrm{span}\{\sigma(1), \sigma(\zeta_m^1), \ldots, \sigma(\zeta_m^{n-1})\}$ and $\|\sigma(\zeta_m^i)\| = \sqrt{n}$. Note that

$$\begin{aligned} \Delta_K &= |\det(\sigma_i(\zeta_m^j))|^2 && (5.33) \\ &= |\det(\mathrm{Tr}(\zeta_m^i \zeta_m^j))|, && (5.34) \end{aligned}$$

because

$$\mathrm{Tr}(x_i x_j) = \sum_k \sigma_k(x_i x_j) = \sum_k \sigma_k(x_i)\sigma_k(x_j) = H^T H,$$

where $x_i = \zeta_m^i$ and $H = (\sigma_i(x_j))$.

$I \subset K$ is called a fractional ideal if $\exists d \in R$ such that $dI \subset R$ is an integral ideal. It is principal if $I = uR$ for some $u \in K$. $\sigma(I) \subset H$ called an ideal lattice. For an $I \subset R$, define the norm as $N(I) = |R/I|$ (= the number of cosets of I in R).

Note the following:

- Consider the lattices $\sigma(R) \supset \sigma(I)$. Then $N(I) = |\sigma(R)/\sigma(I)|$, and $\sigma(R)$ is the $\mathbb{Z}$-span of $\sigma(1), \sigma(\zeta_m^1), \ldots, \sigma(\zeta_m^{n-1})$. $\sigma(\langle a \rangle)$ is spanned by $\sigma(a), \sigma(a\zeta_m^1), \ldots, \sigma(a\zeta_m^{n-1})$. The j-th coordinate $\sigma_j(a\zeta_m^i) = \sigma_j(a)\sigma_j(\zeta_m^i)$ is stretched by $\sigma_j(a)$. Hence, $N(\langle a \rangle) = |N(a)|$.

- $N(aI) = N(I)N(\langle a \rangle)$ because $|R/aI| = |\frac{R}{I}||\frac{I}{aI}| = N(I)N(\langle a \rangle)$ and $|\frac{I}{aI}| = |\frac{R}{aR}|$.

- $N(IJ) = N(J)N(I)$
  (Case 1) I, J coprime
  The Chinese remainder theorem says that $R \to R/I \oplus R/J$ is onto, and its kernel is $I \cap J = IJ$. (It is trivial to see $IJ \subset I \cap J$. To show that $I \cap J \subset IJ$, let $y \in I \cap J$; then $y = y \cdot 1 = y(a + b) = ya(\in IJ) + yb(\in IJ)$, where $a \in I$ and $b \in J$, since $I + J = R$.) Remember that any element of IJ is of the form

$$a_1 b_1 + \cdots + a_l b_l \text{ for } a_i \in I, b_j \in J. \tag{5.35}$$

  (Case 2) $I = p^m, J = p^k$ for some prime ideal p.
  Just note that $R/p \approx p^n/p^{n+1}$. (Since R is Dedekind, p^n/p^{n+1} is singly generated; the isomorphism is given by multiplying the inverse of the generator.)
  (Case 3) The general situation can be reduced to either (Case 1) or (Case 2).

The norm of a fractional ideal I is defined by $N(I) := N(dI)/|N(d)|$, where $d \in R$ is such that $dI \subseteq R$. This is well-defined. Note that $\det(\sigma(I)) = N(I)\sqrt{\Delta_K}$, since $\det \sigma(R) = \sqrt{\Delta_K}$. ($\det \sigma(I)$ is the determinant of the lattice $\sigma(I) \subset H \subset \mathbb{C}^{\mathbb{Z}_m^*}$.)

Lemma 5.4.2.

$$\sqrt{n} N^{1/n}(I) < \lambda_1(I) \leq \sqrt{n} N^{1/n}(I) \sqrt{\Delta_K^{1/n}} \tag{5.36}$$

Proof. The upper bound is just Minkowski's inequality. To prove the lower bound, let $v \in I$ such that $\|v\| = \lambda_1(I)$. Since $\langle v \rangle \subset I$,

$$\mathrm{N}(I) \leq |N(v)| = \left| \prod_i \sigma_i(v) \right|.$$

Note that $\|v\|^2 = \sum |\sigma_i(v)|^2$ by the definition of the metric on H. Also,

$$\left(\prod_i |\sigma_i(v)|^2 \right)^{\frac{1}{n}} \leq \frac{1}{n} \sum_i |\sigma_i(v)|^2. \tag{5.37}$$

Hence, $\sqrt{n} N(I)^{\frac{1}{n}} \leq \|v\|$. □

Remark 5.4.3. It follows that $GapSVP_\gamma$ of ideal lattice is trivial if $\gamma = \mathrm{poly}(n)$.

5.4.4 Duality

For more details, see [Con09].

Definition 6. For a fractional ideal I in K, its dual is defined as

$$I^\vee = \{a \in K : \mathrm{Tr}(aI) \subseteq \mathbb{Z}\}. \tag{5.38}$$

Then $\sigma(T^\vee)$ is a dual lattice (more precisely, a conjugate dual lattice) of $\sigma(I)$, because the inner product in H is defined by Tr.

Definition 7. For any Q-basis $B = \{b_j\}$ of K, define a dual basis $B^\vee = \{b_j^\vee\}$, where $\mathrm{Tr}(b_i b_j^\vee) = \delta_{ij}$.

Note that $R^\vee \supset R$ from the definition of integral elements, because $\mathrm{Tr}(r) \in \mathbb{Z}$ for all $r \in R$.

Lemma 5.4.4. $I^\vee = I^{-1}R^\vee$ ($R^\vee$ is called the codifferent, $(R^\vee)^{-1}$ the different).

Here $I^{-1} := \{x \in K : xI \subset R\}$. It is a fractional ideal.

Proof.

1) $I^{-1}R^\vee \subset I^\vee$: trivial from the definitions of I^{-1}, $R^\vee$ and $I^\vee$.

2) Note that

$$\begin{aligned} \mathrm{N}(I^\vee) &= \left|\frac{R}{I^\vee}\right| && (5.39)\\ &= \left|\frac{I^\vee}{R}\right|^{-1} && (5.40)\\ &= \left|\frac{I^\vee}{R^\vee}\right|^{-1}\left|\frac{R^\vee}{R}\right|^{-1} && (5.41)\\ &= \left|\frac{R}{I}\right|^{-1}\Delta_K^{-1} && (5.42)\\ &= N(I)^{-1}\Delta_K^{-1}, && (5.43) \end{aligned}$$

because $I \subset R \subset R^\vee \subset I^\vee$, $|\frac{I}{J}| = \frac{\det\sigma(J)}{\det\sigma(I)}$, $|\frac{I^\vee}{J^\vee}| = |\frac{J}{I}|^{-1}$, $\det I^\vee = (\det I)^{-1}$, and $\det(\sigma(R)) = \sqrt{\Delta_K}$. Note also

$$\mathrm{N}(I^{-1}R^\vee) = N(I^{-1})N(R^\vee) = N(I)^{-1}\Delta_K^{-1}, \tag{5.44}$$

because $N(IJ) = N(I)N(J)$ holds for general fractional ideals $I, J \subset K$. Hence, $I^\vee = I^{-1}R^\vee$.

□

Lemma 5.4.5. Let m be a power of prime p, $m' = m/p$, and j an integer. Then

$$\mathrm{Tr}(\zeta_m^j) = \begin{cases} \varphi(p)m' & \text{if} \quad j = 0 \mod m, \\ -m' & \text{if} \quad j = 0 \mod m', \quad j \neq 0 \mod m, \\ 0 & \text{otherwise}. \end{cases} \tag{5.45}$$

Proof. Let $d = gcd(j, m)$, $\tilde{m} = m/d$. Then

$$\mathrm{Tr}(\zeta_m^j) = \sum_{\alpha\in\mathbb{Z}_m^*}(\zeta_m^j)^\alpha = \sum_{\alpha\in\mathbb{Z}_m^*}(\zeta_m^{dj'})^\alpha, \tag{5.46}$$

where $j = dj'$. If $\alpha = \alpha' \mod (m/d = \tilde{m})$, $dj'\alpha' = dj'(\alpha + \frac{m}{d}k) = dj'\alpha + j'mk$. Hence, $\zeta_m^{dj'\alpha} = \zeta_m^{dj'\alpha'}$. Therefore we have

$$\mathrm{Tr}(\zeta_m^j) = d\ \mathrm{Tr}_{Q(\zeta_{\tilde{m}})}(\zeta_{\tilde{m}}^{j/d}), \tag{5.47}$$

since we have d such α's, and $\zeta_m^d = \zeta_{\tilde{m}}$.

Note that $\mathbb{Z}_m^* \to \mathbb{Z}_{\tilde{m}}^*$ is d-fold onto map when $m = d\tilde{m}$. Also note that

$$\sum_{i \in \mathbb{Z}_m^*} \omega_m^i = \begin{cases} -1 & \text{if } m = p, \\ 0 & \text{if } m = p^k, k \geq 2, \end{cases} \tag{5.48}$$

where ω_m is a primitive mth root of unity, because

$$\Phi_p(x) = 1 + x + \cdots + x^{p-1} \tag{5.49}$$
$$\Phi_m(x) = 1 + x^{m'} + \cdots + x^{m'(p-1)} \tag{5.50}$$

where $m' = p^{k-1}$. The lemma follows, because $\zeta_{\tilde{m}}^{j/d}$ is a primitive $\tilde{m}$-th root of unity. $\square$

Lemma 5.4.6. Let m be a power of a prime p, $m' = m/p$, and let $g = 1 - \zeta_p \in R = \mathbb{Z}[\zeta_m]$. Then $R^\vee = \left\langle \frac{g}{m} \right\rangle$, $p/g \in R$, and $\langle g \rangle$ and $\langle p' \rangle$ are coprime for every prime integer $p' \neq p$.

Proof. We first show that $g/m \in R^\vee$. It suffices to show that $\mathrm{Tr}(\zeta_m^j g/m)$ is an integer for every $j \in [\varphi(m)]$. Note that

$$\zeta_m^j g/m = (\zeta_m^j - \zeta_m^{j+m'})/m. \tag{5.51}$$

$$\mathrm{Tr}(\zeta_m^j - \zeta_m^{j+m'}) = \begin{cases} (\phi(p)+1)m'(= m) & \text{if } j = 0 \mod m, \\ (-m') - (-m') = 0 & \text{if } j = 0 \mod m' \text{ and } j \neq 0 \mod m, \\ 0 & \text{otherwise.} \end{cases}$$

Note that in the second case, $j \in [\varphi(m)]$, i.e., $j = 0, \cdots, m'(p-1) - 1$, hence not only j but also $j + m$ satisfies $j = 0 \mod m'$ and $j \neq 0 \mod m$.

We therefore have

$$\mathrm{Tr}(\zeta_m^j g/m) = \begin{cases} 1 & \text{for } j = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{5.52}$$

To show $R^\vee = \langle g/m \rangle$, we compute $N(R^\vee)$ and $N(g/m)$. Let $m = p^l$.

$$\mathrm{N}(R^\vee) = \Delta_K^{-1} \quad \text{(by Eq. (5.44))} \tag{5.53}$$
$$= \left(\frac{p^{\frac{1}{p-1}}}{p^l} \right)^{p^{l-1}(p-1)} = \frac{p^{p^{l-1}}}{m^{\varphi(m)}} = \frac{p^{m/p}}{m^{\varphi(m)}} \tag{5.54}$$
$$\tag{5.55}$$
$$\mathrm{N}(m) = m^{\varphi(m)} \tag{5.56}$$
$$\tag{5.57}$$
$$\mathrm{N}(g) = \mathrm{N}(1 - \zeta_p) = [N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1 - \zeta_p)]^{m/p} \tag{5.58}$$
$$= [(1 - \zeta_p)(1 - \zeta_p^2) \cdots (1 - \zeta_p^{p-1})]^{m/p} \tag{5.59}$$
$$= p^{m/p} \tag{5.60}$$

since

$$\Phi_p(x) = (x - \zeta_p) \cdots (x - \zeta_p^{p-1}) = 1 + x + \cdots + x^{p-1},$$

and letting $x = 1$, we obtain $(1 - \zeta_p)(1 - \zeta_p^2) \cdots (1 - \zeta_p^{p-1}) = p$. Hence

$$\mathrm{N}(g/m) = N(g)N(m)^{-1} = p^{m/p} \cdot m^{-\varphi(m)} = N(R^\vee), \tag{5.61}$$

i.e., $R^\vee = \langle \frac{g}{m} \rangle$.
To prove $p/g \in R$, note that

$$(1-\zeta_p)((p-1)+(p-2)\zeta_p+\cdots+2\zeta_p^{p-3}+\zeta_p^{p-2}) \tag{5.62}$$
$$= (p-1)-(\zeta_p+\zeta_p^2+\cdots+\zeta_p^{p-1}) = p, \tag{5.63}$$

$$p/g = p/(1-\zeta_p) \in R. \tag{5.64}$$

To show that $\langle g\rangle$ and $\langle p'\rangle$ are coprime for every prime integer $p' \neq p$, note that $N(\langle g\rangle) = p^{m/p}$, power of p. Since the norm of $\langle g\rangle + \langle p'\rangle$ is a divisor of both a power of p and of p', it must be 1, implying that $\langle g\rangle$ and $\langle p'\rangle$ are coprime. □

Remark 5.4.7.

$$\left|\frac{R}{\langle g\rangle + \langle p'\rangle}\right| = \left|\frac{R}{\langle g\rangle}\right|\left|\frac{\langle g\rangle}{\langle g\rangle + \langle p'\rangle}\right| \tag{5.65}$$
$$= \left|\frac{R}{\langle g\rangle}\right|\left|\frac{\langle g\rangle + \langle p'\rangle}{\langle g\rangle}\right|^{-1} \tag{5.66}$$

Hence, it is a factor of $\left|\frac{R}{\langle g\rangle}\right| = p^{m/p}$, i.e., a power of p.
On the other hand,

$$\left|\frac{R}{\langle g\rangle + \langle p'\rangle}\right| = \left|\frac{R}{\langle p'\rangle}\right|\left|\frac{\langle p'\rangle}{\langle g\rangle + \langle p'\rangle}\right| \tag{5.67}$$
$$= \left|\frac{R}{\langle p'\rangle}\right|\left|\frac{\langle g\rangle + \langle p'\rangle}{\langle p'\rangle}\right|^{-1}, \tag{5.68}$$

so it is a factor of $\left|\frac{R}{\langle p'\rangle}\right| = p'^{\varphi(m)}$.

Definition 8. If $m = \prod_l m_l$ is a product of powers of distinct primes, define $g = \prod_p (1-\zeta_p)$, where p is an odd prime factor of m. For $R = \mathbb{Z}[\zeta_m] = \bigotimes_l \mathbb{Z}[\zeta_{m_l}]$, let $t = \hat{m}/g \in R$, where $\hat{m} = m/2$ if m even, and $\hat{m} = m$ otherwise.

Note that $\hat{m}/g \in R$ because $(1-\zeta_2) = 2$, so $\hat{m}/g = m/\prod_p(1-\zeta_p) \in R$, where p runs over all primes dividing m.

Corollary 5.4.8. $R^\vee = \langle g/\hat{m}\rangle = \langle t^{-1}\rangle$, and $\langle g\rangle$ is coprime with $\langle p'\rangle$ for every prime integer p' except the odd primes dividing m.

Proof. Just note that $R \cong \bigotimes_l R_l$, where $R_l = \mathbb{Z}[\zeta_{m^l}]$ and $g = \otimes g_l$, where $g_l = 1 - \zeta_{p_l}$.

$$R^\vee = \otimes_l R_l^\vee = \otimes_l \frac{g_l}{m_l} R_l = \frac{g}{\hat{m}} \otimes_l R_l. \tag{5.69}$$

□

5.4.5 Prime Splitting and Chinese Remainder Theorem

For an integer prime $p \in \mathbb{Z}$, the factorization of principal ideal $\langle p\rangle \subset R = \mathbb{Z}[\zeta_m]$ is as follows. Let p^d be a prime factor of m, let $h = \varphi(p^d)$, $f =$ the multiplicative order of p modulo m/p^d. Then $\langle p\rangle = \mathfrak{p}_1^h \cdots \mathfrak{p}_g^h$, where $g = \frac{n}{hf}$, $n = \varphi(m)$, and $\mathfrak{p}_i$ are distinct primes in R, each of norm p^f. ($n = \varphi(m) = \varphi(p^d)\varphi(m')$, $m' = m/p^d$, $p^f = 1 \mod m'$. Hence, $f|\varphi(m')(= n/h)$. Also, $N(\langle p\rangle) = p^n$ and $N(p_1^h \cdots p_g^h) = p^{fgh} = p^n$.) In particular, if prime $q = 1 \mod m$, so that q is larger than m, then $h = 1$ and $f = 1$, hence $\langle q\rangle$ splits completely into n distinct prime ideals of norm q in R. Notice that the field $\mathbb{Z}_q$ has a primitive mth root of unity, ω_m, because the multiplicative subgroup of $\mathbb{Z}_q$ is cyclic with order $q-1$, which is a multiple of m. Note that $\omega_m^i \in \mathbb{Z}_q$, where $i \in \mathbb{Z}_m^*$, are also distinct mth roots of unity. Then the prime ideal factors of $\langle q\rangle$ are $q_i = \langle q\rangle + \langle \zeta_m - \omega_m^i\rangle$. Hence, each quotient ring R/q_i is isomorphic to $\mathbb{Z}_q$ via the map $\zeta_m \mapsto \omega_m^i$, which confirms $N(q_i) = q$. In this case,

$$\frac{\mathbb{Z}[\zeta_m]}{\langle q\rangle} = \mathbb{Z}_q[\zeta_m] = \frac{\mathbb{Z}_q[x]}{\Phi_m(x)} = \bigoplus_{i\in\mathbb{Z}_m^*} \frac{\mathbb{Z}_q[x]}{x-\omega_m^i} \approx (\mathbb{Z}_q)^n.$$

(Note that $\Phi_m(x) = \prod_{i\in\mathbb{Z}_m^*}(x-\omega_m^i)$, where $\omega_m^i \in \mathbb{Z}_q$, and $\frac{\mathbb{Z}_q[x]}{x-\omega_m^i} \approx \mathbb{Z}_q$ for each $i \in \mathbb{Z}_m^*$, because $\mathbb{Z}_q + \omega_m^i\mathbb{Z}_q = \mathbb{Z}_q$.)

5.5 Ring-LWE

The formal definition of the ring-LWE problem is provided and the worst-case hardness result in [LPR10] is shown as follows.

Definition 9 (Ring-LWE Distribution)**.** For a secret $s \in R_q^\vee$ (or $R^\vee$) and a distribution ψ over $K_{\mathbb{R}} = K \otimes \mathbb{R}$, which is isomorphic to H via σ, a sample from the ring-LWE distribution, $A_{s,\psi}$, over $R_q \times (K_{\mathbb{R}}/qR^\vee)$ is generated by choosing $a \leftarrow R_q$ uniformly at random, choosing $e \leftarrow \psi$ and outputting $(a, b = a\cdot s + e \mod qR^\vee)$.

Definition 10 (Ring-LWE, Average-Case Decision)**.** The average-case decision version of the ring-LWE problem, denoted $R - DLWE_{q,\psi}$, is to distinguish with nonnegligible advantage between independent samples from $A_{s,\psi}$, where $s \leftarrow R_q^\vee$ uniformly random, and the same number of uniformly random and independent samples from $R_q \times (K_{\mathbb{R}}/qR^\vee)$.

Theorem 5.5.1. Let K be the mth cyclotomic number field having dimension $n = \varphi(m)$, and R its ring of integers. Let $\alpha = \alpha(n) > 0$ and let $q = q(n) \geq 2$, $q = 1 \mod m$ be a poly(n)-bounded prime such that $\alpha q \geq \omega(\sqrt{\log n})$. (Note that $f = \omega(g)$ if $g = o(f)$.) Then there is a polynomial-time quantum reduction from $\tilde{O}(\sqrt{n}/\alpha)$-approximate SVIP (or SVP) on ideal lattices in K to the problem of solving $R - DLWE_{q,\psi}$ given only l samples, where ψ is the Gaussian distribution $D_{\xi q}$ for $\xi = \alpha\cdot(nl/\log(nl))^{1/4}$.

Lemma 5.5.2 (Discretization)**.** Let p and q be positive coprime integers, and $\lfloor\rceil$ a valid discretization, defined earlier, to cosets of $pR^\vee$. Let $w \in R_p^\vee$ and $(a', b') \in R_q \times K_{\mathbb{R}}/qR^\vee$. Output $(a = pa' \mod qR, b) \in R_q \times R_q^\vee$, where $b = \lfloor pb'\rceil_{w+pR^\vee} \mod qR^\vee$. If $(a', b') \in A_{s,\psi}$, then $(a, b) \in A_{s,\chi}$ where the error distribution χ is $\lfloor p\psi\rceil_{w+pR^\vee}$. If (a', b') is uniformly random, then so is (a, b).

We show that the following variant of ring-LWE is as hard as the original one, closely following the technique of [ACPS09].

Lemma 5.5.3 (Normal form of $R-LWE$)**.** Let p and q be positive coprime integers, $\lfloor\rceil$ a valid discretization to cosets of $pR^\vee$, and $w \in R_p^\vee$. If $R - LWE_{q,\psi}$ is hard given some number l of samples, then so is the variant of $R - LWE_{q,\psi}$ in which the secret is sampled from $\chi := \lfloor p\psi\rceil_{w+pR^\vee}$, given $l-1$ samples.

Proof. Start by drawing one sample and apply discretization to obtain 0th sample (a_0, b_0). Let us assume that the 0th sample $(a_0, b_0) \in R_q \times R_q^\vee$ is such that a_0 is invertible i.e., $a_0 \in R_q^*$. From $l-1$ samples $(a_i, b_i) \in R_q \times K_{\mathbb{R}}/qR^\vee$, $(i = 1, \ldots, l-1)$, output

$$(a_i' = -a_0^{-1}a_i, b_i' = b_i + a_i'b_0) \in R_q \times K_{\mathbb{R}}/qR^\vee. \tag{5.70}$$

This is the same kind of reduction we used to obtain the normal form of standard LWE. If (a_i, b_i) is uniform, so is (a_i', b_i'). If $(a_i, b_i) \in A_{s,\psi}$, then for each i,

$$\begin{aligned} b_i' &= (a_i \cdot s + e_i) - a_0^{-1}a_i(a_0 \cdot s + e_0) && (5.71)\\ &= a_i'e_0 + e_i, && (5.72) \end{aligned}$$

where e_0 is our secret. Once we find e_0, we obtain s from $b_0 = a_0 \cdot s + e_0$. $\square$

Remark 5.5.4. When $R = \mathbb{Z}[\zeta_m]$, the fraction of invertible elements in R_q is at least $1/\operatorname{poly}(n, \log q)$ (see the [LPR10]).

Note: As in $\mathbb{Z}$, for prime ideal p of R, an elements $a \in R$ is invertible modulo p^r if and only if $a \neq 0 \mod p$. Hence, the fraction of noninvertible elements in R/p^r is $\left|\frac{R}{\langle p\rangle}\right|^{-1} = 1/N(p)$.

The proof of Remark 5.5.4 goes as follows.
Let $q = p_1^{l_1} \cdots p_\alpha^{l_\alpha}$ be a prime-power factorization of q. Then

$$\frac{R}{\langle q\rangle} = \bigoplus_{\text{prime } p|q} \frac{R}{\langle p^{l_p}\rangle}.$$

Note that the fraction of noninvertible elements in $\frac{R}{\langle p^{l_p}\rangle}$ is equal to that of $\frac{R}{\langle p\rangle}$. Since $\langle p\rangle = p_1^h \cdots p_g^h$ in R, where $h = \varphi(p^d)$, f the multiplicative order of p modulo m/p^d, p^d the largest power of p that divides m, $g = n/(hf)$, $R = \mathbb{Z}[\zeta_m]$, $n = \varphi(m)$, and $N(p_i) = p^f$. Hence,

$$\prod_{\text{prime } p|q} (1 - p^{-f_p})^{\frac{n}{f_p\varphi(p^{d_p})}} \geq \prod_{\text{prime } p|q} (1 - p^{-f_p})^{\frac{n}{\varphi(p^{d_p})}}. \tag{5.73}$$

Since $p^{f_p} = 1 \mod (m/p^{d_p})$, $p^{f_p} \geq \frac{m}{p^{d_p}} + 1$, so

$$\begin{aligned} (1 - p^{-f_p})^{\frac{n}{\varphi(p^{d_p})}} &= (1 - p^{-f_p})^{\varphi(\frac{m}{p^{d_p}})} && (5.74)\\ &\geq (1 - p^{-f_p})^{\frac{m}{p^{d_p}}} && (5.75)\\ &\geq e^{-1}, && (5.76) \end{aligned}$$

using $(1 - \frac{1}{1+x})^x > e^{-1}$ when $x > 0$. Note that the number of primes diving m is less than $\log_2 m$. ($\because$ Let $m = p_1^{l_1} \cdots p_k^{l_k}$, then $\log_2 m = l_1 \log_2 p_1 + \cdots + l_k \log_2 p_k > k$ since $l_i \geq 1$, $\log_2 p_i > 1$.) Hence, the above product restricted to p which divides both m and q is greater than $\left(\frac{1}{e}\right)^{\log_2 m} = \frac{1}{\operatorname{poly}(m)}$. If the prime p does not divide m, $d_p = 0$. Hence, in this case, we compute $\prod_{p|q, p\nmid m} (1 - p^{-f_p})^n$ because $\varphi(p^{d_p}) = 1$. Since p^{f_p} are distinct for distinct p and $p^{f_p} \equiv 1$ modulo m, it is bounded below by

$$\prod_{k=1}^{\log_2 q} \left(1 - \frac{1}{km+1}\right)^n \geq \prod_{k=1}^{\log_2 q} e^{-n/km} \quad \left(\because 1 - \frac{1}{\alpha+1} \geq e^{-\frac{1}{\alpha}}\right) \tag{5.77}$$

$$\geq \prod_{k=1}^{\log_2 q} e^{-1/k} \quad (\because n = \varphi(m) < m) \tag{5.78}$$

$$\geq e^{-1} \prod_{k=2}^{\log_2 q} \left(1 - \frac{1}{k}\right) \tag{5.79}$$

$$= (e \log_2 q)^{-1}. \quad \left(\because \frac{1}{2} \cdot \frac{2}{3} \cdots \frac{l-1}{l} = \frac{1}{l}\right) \tag{5.80}$$

Thus we have shown that the fraction of invertible elements is greater than $\frac{1}{\mathrm{poly}(n, \log q)}$.

We used the following fact:

$$\left(\frac{1+x}{x}\right)^x = \left(1 + \frac{1}{x}\right)^x \nearrow e \swarrow \left(1 + \frac{1}{x}\right)^{x+1}$$

Hence,

$$\left(1 - \frac{1}{1+x}\right)^x = \left(\frac{x}{1+x}\right)^x \searrow e^{-1},$$

therefore $1 - \frac{1}{1+x} > e^{-1/x}$ for all $x > 0$.

Chapter 6

Discrete Fourier Transform & Chinese Remainder Transform

We follow the algebraic framework of [LPR13].

- ω_m: a primitive mth root of unity.
- m: prime power.
- DFT_m: $\mathbb{Z}_m \times \mathbb{Z}_m$ matrix whose (i,j)th entry is ω_m^{ij} $(i,j = 0,1,\cdots,m-1)$.
- CRT_m: submatrix of DFT_m obtained by restricting to the rows indexed by $\mathbb{Z}_m^*$ and columns indexed by $[\varphi(m)]$.

For any positive integer with prime factorization $m = \prod_l m_l$,

$$DFT_m := \bigotimes_l DFT_{m_l}, \quad CRT_m := \bigotimes_l CRT_{m_l}. \tag{6.1}$$

Remark 6.0.5. DFT is unitary up to scaling by $\sqrt{n}$, while CRT not unitary even up to scaling.

Decomposition of DFT_m when m is a prime power (Fast Fourier Transform (FFT))

Let $m' = m/p$. We reindex columns of the matrix by $j \leftrightarrow (j_0, j_1) \in [p] \times [m']$ such that $j = m'j_0 + j_1$ and rows of the matrix by $i \leftrightarrow (i_0, i_1) \in [p] \times [m']$ such that $i = pi_1 + i_0$. (Remark: Let $m = p^k$ and write $n = \alpha_{k-1}\cdots\alpha_1\alpha_0$ in p-digit representation, i.e., $n = \alpha_0 + p\alpha_1 + \cdots + p^{k-1}\alpha_{k-1}$. Then for $n = \alpha_{k-1}\alpha_{k-2}\cdots\alpha_1\alpha_0$, $j_0 = \alpha_{k-1}$, $j_1 = \alpha_{k-2}\cdots\alpha_1\alpha_0$, $i_0 = \alpha_0$, $i_1 = \alpha_{k-1}\cdots\alpha_1$.) Then we claim

$$DFT_m = (I_{[p]} \otimes DFT_{m'}) \cdot T_m \cdot (DFT_p \otimes I_{[m']}), \tag{6.2}$$

where T_m is a "diagonal" matrix having $\omega_m^{i_0 i_1}$ in the $((i_0,i_1),(i_0,i_1))$th diagonal entry. Note that diagonal in this new setting is not diagonal in the standard convention. But T_m is at least unitary. Also, the matrix multiplication is defined with respect to the new column-row index system, i.e., $(AB)_{(i_0,i_1)}^{(j_0,j_1)} = \sum_{\beta=0}^{m'-1}\sum_{\alpha=0}^{p-1} A_{(i_0,i_1)}^{(\alpha,\beta)} B_{(\alpha,\beta)}^{(j_0,j_1)}$.

Proof. Let $I_{[p]} \otimes DFT_{m'} = A$, $T_m = B$, and $DFT_p \otimes I_{[m']} = C$. Then it suffices to show that

$$(DFT_m)^{(j_0,j_1)}_{(i_0,i_1)} = A^{(i_0,j_1)}_{(i_0,i_1)} B^{(i_0,j_1)}_{(i_0,j_1)} C^{(j_0,j_1)}_{(i_0,j_1)} \tag{6.3}$$

because of the definitions of A, B, C. Just note that

$$\omega_{m'}^{i_1 j_1} \omega_m^{i_0 j_1} \omega_p^{i_0 j_0} = \omega_m^{m' i_0 j_0 + i_0 j_1 + p i_1 j_1} = \omega_m^{(p i_1 + i_0)(m' j_0 + j_1)}. \tag{6.4}$$

□

Similarly, we have

$$CRT_m = (I_{\mathbb{Z}_p^*} \otimes DFT_{m'}) \hat{T}_m (CRT_p \otimes I_{[m']}). \tag{6.5}$$

CRT_m is the submatrix of DFT_m restricted to the rows $\mathbb{Z}_p^* \times [m']$ and the columns $[\varphi(p)] \times [m']$, because $\mathbb{Z}_m^* \cong \mathbb{Z}_p^* \times [m']$ and $\varphi(m) = \varphi(p) \cdot m'$.

- $\mathbb{Z}_p^* \times [m'] \leftrightarrow i = p i_1 + i_0 \in \mathbb{Z}_m^*$ since $i_0 = 1, \cdots, p-1$, and $i \in \mathbb{Z}_m^*$ if and only if i is not a multiple of p.
- $[\varphi(p)] \times [m'] \leftrightarrow \{0, \ldots, (p-2)m' + (m'-1) = pm' - m' - 1 = \varphi(m) - 1\}$
  $((j_0, j_1) \leftrightarrow j = m' j_0 + j_1, j_0 = 0, \cdots, p-2 = \varphi(p) - 1)$

Chapter 7

Powerful basis

7.1 Powerful basis $\vec{p}$ of $K = Q(\zeta_m)$ and $R = \mathbb{Z}[\zeta_m]$

- For a prime power m, $\vec{p}^T = (\zeta_m^j)_{j\in[\varphi(m)]}$, a vector over R.
- For m with prime power factorization $m = \prod m_l$, $\vec{p} = \otimes_l \vec{p_l}$.
- For $I = (R^\vee)^k \subset K$ of $R^\vee = \langle t^{-1}\rangle$, the powerful basis of I is $t^{-t}\vec{p}$.

Remark 7.1.1. Note that for $p_{(j_l)} = \otimes_l \zeta_{m_l}^{j_l}$, we have, from $\zeta_{m_l} = \zeta_m^{(m/m_l)j_l}$,

$$p_{(j_l)} \leftrightarrow \prod_l \zeta_m^{(m/m_l)j_l}. \tag{7.1}$$

For example, when $m = 15$, $\zeta = \zeta_{15}$ for $(j_1, j_2) \in [\varphi_{(3)}] \times [\varphi_{(5)}] \leftrightarrow \zeta_{15}^{5j_1+3j_2}$, $[\varphi(3)] = \{0,1\}$, $[\varphi(5) = \{0,1,2,3\}]$, the powerful basis consists of

$$\zeta^0 \leftarrow (0,0), \zeta^3 \leftarrow (0,1), \zeta^5 \leftarrow (1,0), \zeta^6 \leftarrow (0,2), \tag{7.2}$$
$$\zeta^8 \leftarrow (1,1), \zeta^9 \leftarrow (0,3), \zeta^{11} \leftarrow (1,2), \zeta^{14} \leftarrow (1,3), \tag{7.3}$$

which are different from the power basis $\{\zeta^0, \zeta^1, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6, \zeta^7\}$.

Applying the canonical embedding σ, we obtain a $\mathbb{Z}_m^*$-by-$\varphi(m)$ matrix

$$\left(\boxed{\sigma(\zeta_m^0)} \quad \boxed{\sigma(\zeta_m^1)} \quad \cdots \quad \boxed{\sigma(\zeta_m^{\varphi(m)-1})} \right) \tag{7.4}$$

which is nothing but CRT_m, i.e., $\sigma(\vec{p}^T) = CRT_m$ when m is a prime power.

<u>Claim:</u> $\|p_j\|_\infty = 1$ and $\|p_j\|_2 = \sqrt{\varphi(m)} = \sqrt{n}$ for all p_j.

If $m = p^k$,

$$\vec{p}^T = (1, \zeta_m, \zeta_m^2, \cdots, \zeta_m^{p^{k-1}(p-1)-1}), \tag{7.5}$$

and $\sigma(\vec{p}^T)$ is a $\mathbb{Z}_m^* \times [\varphi(m)]$ matrix such that

$$\sigma(\vec{p}^T) = \begin{pmatrix} 1 & \omega_m & & \cdots & \\ 1 & \omega_m^2 & & & \\ \vdots & \vdots & & & \\ 1 & & & & \\ 1 & & & & \end{pmatrix} = CRT_m, \tag{7.6}$$

because $\sigma(\zeta_m) = \begin{pmatrix} \omega_m \\ \vdots \\ \omega_m^i \\ \vdots \end{pmatrix}$, where $i \in \mathbb{Z}_m^*$.

Remark 7.1.2. $\sigma(\vec{p}^T)$ is not unitary even up to scaling because $\sigma(p_j)$s are not orthogonal to each other, which is same as saying that CRT_m is not unitary. Remember that DFT_m is unitary up to scaling.

Lemma 7.1.3. The largest singular value of $\sigma(\vec{p}^T)$ is $s_1(\vec{p}) = \sqrt{\hat{m}}$ and the smallest singular value is $s_n(\vec{p}) = \sqrt{\frac{m}{\mathrm{rad}(m)}}$.

Remark 7.1.4. $\hat{m} = m/2$ if m is even, otherwise $\hat{m} = m$. Note that the ratio of $s_1(\vec{p})$ to $\sqrt{\varphi(m)}$ is just $\sqrt{\hat{m}/\varphi(m)} = (\prod_p \frac{p}{p-1})^{1/2} = \mathcal{O}(\sqrt{\log\log m})$, where the product runs over all odd primes dividing m. Note that

$$\prod_{\substack{p|m \\ \text{prime}}} \frac{p}{p-1} \approx 1 + \sum_{\substack{p|m \\ \text{prime}}} \frac{1}{p} \leq 1 + \sum_{n=1}^{\log_2 m} \frac{1}{n} \approx 1 + \int_1^{\log_2 m} \frac{1}{x} dx \approx \log(\log m), \tag{7.7}$$

and that $(\det R)^{\frac{1}{n}} = \Delta_K^{\frac{1}{2\varphi(m)}} \leq \sqrt{\varphi(m)}$. Hence, $\vec{p}$ is a relatively good basis, since $\frac{s_1(\vec{p})}{\|p_j\|}$ is $\mathcal{O}(\sqrt{\log\log m})$.

Proof. We may assume that m is a power of a prime p. Let $m' = m/p$. Then

$$CRT_m = (\sqrt{m'}Q)(CRT_p \otimes I_{[m']}) \tag{7.8}$$

for some unitary Q, because $DFT_{m'}/\sqrt{m'}$ is unitary and so is the $\hat{T_m}$. Hence, it suffices to copute the singular values of CRT_p. Note that

$$CRT_p^* CRT_p = (pI_{[\varphi(p)]} - \mathbb{1} \cdot \mathbb{1}^T). \tag{7.9}$$

In particular, CRT_p is not unitary even up to scaling. To prove this, the first $[\varphi(p)]$ columns of DFT_p is $A := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ & & CRT_p & \end{pmatrix}$. Then

$$A^* A = \begin{pmatrix} 1 & \\ 1 & \\ \vdots & CRT_p^* \\ 1 & \end{pmatrix} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ & & CRT_p & \end{pmatrix} = pI_{[\varphi(p)]}, \tag{7.10}$$

because the columns of DFT_p are orthogonal to each other and has length $\sqrt{p}$. Also note that

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ & & 0 & \end{pmatrix} + \begin{pmatrix} 0 & 0 & \cdots & 0 \\ & & CRT_p & \end{pmatrix}. \tag{7.11}$$

Then

$$pI_{[\varphi(p)]} = A^* A = CRT_p^* CRT_p + \mathbb{1} \cdot \mathbb{1}^T. \tag{7.12}$$

The eigenvalues and the corresponding eigenvectors of $(pI_{[\varphi(p)]}) - \mathbb{1} \cdot \mathbb{1}^T$ are $p \leftrightarrow (1, -1, 0, \cdots, 0), \cdots, p \leftrightarrow (1, 0, \cdots, -1)$, $(p-2)$ times, and $1 \leftrightarrow (1, 1, \cdots, 1)$. □

7.2 Gram-Schmidt orthogonalization of CRT_m

Lemma 7.2.1. Let m be a power of a prime p and $m' = m/p$. Then

$$CRT_m = Q_m(\sqrt{m'} D_p \otimes I_{[m']})(U_p \otimes I_{[m']}), \tag{7.13}$$

where Q_m is unitary, D_p is a real diagonal $[\varphi(p)]$-by-$[\varphi(p)]$ matrix with $\sqrt{(p-1) - j/(p-j)}$ in its j-th diagonal entry, and U_p is an upper unitriangular $[\varphi(p)]$-by-$[\varphi(p)]$ matrix with $-1/(p-i-1)$ in its (i, j)th entry $0 \le i < j < \varphi(p)$.

Proof. We know that

$$CRT_m = \sqrt{m'} Q' (CRT_p \otimes I_{[m']}) \tag{7.14}$$

for some unitary Q'. Thus, it suffices to show that $CRT_p = Q_p D_p U_p$ for some unitary Q_p. We compute

$$G = CRT_p^* CRT_p = (pI_{[\varphi(p)]} - \mathbb{1} \cdot \mathbb{1}^T). \tag{7.15}$$

G has diagonal entries $p - 1$, and -1 elsewhere. From the uniqueness of Cholesky decomposition of G, it suffices to show that $G = U_p^T D_p^2 U_p$, where

$$D_p = \begin{pmatrix} \ddots & & 0 \\ & \sqrt{p-1-j/p-j} & \\ 0 & & \ddots \end{pmatrix}, \tag{7.16}$$

$$U_p = \begin{pmatrix} 1 & -\frac{1}{p-1} & -\frac{1}{p-1} & \cdots & -\frac{1}{p-1} \\ 0 & 1 & -\frac{1}{p-2} & \cdots & -\frac{1}{p-2} \\ 0 & 0 & 1 & & \\ & & & \ddots & \\ & & & & \end{pmatrix}. \tag{7.17}$$

Let us compute the ith ($i \in [\varphi(p)]$) diagonal entry in $U_p^T D_p^2 U_p$, which is

$$
\begin{aligned}
& \sum_j (U_p)_{ji}(D_p^2)_{jj}(U_p)_{ji} && (7.18)\\
= \;& \sum_j (U_p)_{ji}^2 (D_p^2)_{jj}, && (7.19)\\
& \text{and because of triangularity of } U_p, \text{ we obtain} \\
= \;& p - 1 - \frac{i}{p-i} + \sum_{k=0}^{i-1} \frac{1}{(p-k-1)^2}\left(p - 1 - \frac{k}{p-k}\right) && (7.20)\\
= \;& p - 1 - \frac{i}{p-i} + p\sum_{k=0}^{i-1} \frac{1}{(p-k)(p-k-1)} && (7.21)\\
= \;& p - 1 - \frac{i}{p-i} + p(T(p) - T(p-i)) && (7.22)\\
& \left(\text{where } T(k) := \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{(k-1)k} = 1 - \frac{1}{k}\right) \\
= \;& p - 1 - \frac{i}{p-i} + p(1 - \frac{1}{p} - 1 - \frac{1}{p-i}) && (7.23)\\
= \;& p - 1. && (7.24)
\end{aligned}
$$

Computation of the off-diagonal entries is more complicated, but can be done in essentially the same way. □

Chapter 8

Chinese Remainder Basis and Fast Ring Operation

- Note that $\sigma(\vec{p}^T) = CRT_m$, hence if $a = \langle \vec{p}, \mathbf{a} \rangle$, then $\sigma(a) = CRT_m\mathbf{a}$.
- Now assume that q is a prime integer $= 1 \mod m$. In this case, $\dfrac{R}{\langle q \rangle} = \bigoplus_{i \in \mathbb{Z}_m^*} \dfrac{R}{\langle q_i \rangle}$, where $q_i = \langle q \rangle + \langle \zeta_m - \omega_m^i \rangle$ and ω_m is some fixed element of order m in $\mathbb{Z}_q$.

Definition 11. Chinese remainder (or CRT) $\mathbb{Z}_q$-basis $\vec{c}$ of R_q is defined as follows:

- For a prime power m, $\vec{c} = (c_i)_{i \in \mathbb{Z}_m^*}$, where $c_i = 1 \mod q_i$, $c_i = 0 \mod q_j$, $j \neq i$ (The existence of such c_i is guaranteed by the Chinese Remainder Theorem).
- For m having prime-power factorization $m = \prod_l m_l$, define $\vec{c} = \otimes_l \vec{c}_l$.

For any power $I = (R^\vee)^k$ of $R^\vee = \langle t^{-1} \rangle$, we define $t^{-k}\vec{c}$ as the CRT $\mathbb{Z}_q$-basis of I_q.

Note that the ring operation can be done componentwise if the elements are represented in the CRT basis, i.e., if $a = \langle \vec{c}, \mathbf{a} \rangle$ and $b = \langle \vec{c}, \mathbf{b} \rangle \in R_q$, then the coefficient vector of $a \cdot b$ with respect to the CRT basis is componentwise multiplication $\mathbf{a} \odot \mathbf{b}$ over $\mathbb{Z}_q$ by the defining property of $\vec{c}$. When m is a prime power, the CRT basis $\vec{c}$ and the powerful basis $\vec{p} = (\zeta_m^j)_{i \in [\varphi(m)]}$ are related by

$$\vec{p}^T = \vec{c}^T CRT_m, \tag{8.1}$$

i.e., $\zeta_m^j = \sum_{i \in \mathbb{Z}_m^*} c_i \omega_m^{ij}$. To show this identity, just evaluate both sides at q_i. Then both are ω_m^{ij}. They are equal at all of q_i, so they are the same. Hence, if $a \in R_q$ has the coefficient vector $\mathbf{a} \in Z_q^{[\varphi(m)]}$ in the powerful basis, i.e., $a = \langle \vec{p}, \mathbf{a} \rangle$, then its coefficient vector in the CRT basis is $CRT_m\mathbf{a}$, i.e., $a = \langle \vec{c}, CRT_m\mathbf{a} \rangle$.

Chapter 9

Decoding Basis of $R^\vee$

Let τ be an automorphism of R that maps ζ_m to $\zeta_m^{-1} = \zeta_m^{m-1}$. τ is called the conjugation map since $\sigma(\tau(a)) = \overline{\sigma(a)}$. For example, if $\zeta_m \to e^{2\pi i/m}$, then $\zeta_m^{-1} \mapsto e^{-2\pi i/m} = \overline{e^{2\pi i/m}}$. Note that $\tau(\vec{p})$ is also a $\mathbb{Z}$-basis of R.

Definition 12. The decoding basis of $R^\vee$ is $\vec{d} = \tau(\vec{p})^\vee$, the dual of the conjugate of the powerful basis $\vec{p}$.

Remark 9.0.2. Since $R \subset R^\vee \subset K_{\mathbb{R}}$ and $\vec{d}$ is a basis of $R^\vee$, any $a \in K_{\mathbb{R}}$ can be represented in the decoding basis as $a = \left\langle \vec{d}, \mathbf{a} \right\rangle$ for some real vector $\mathbf{a}$. Then

$$a_j = \mathrm{Tr}(a d_j^\vee) = \mathrm{Tr}(a\tau(p_j)) = \langle \sigma(a), \sigma(p_j) \rangle \quad \Longleftrightarrow \quad \mathbf{a} = CRT_m^* \sigma(a), \tag{9.1}$$

because $\sigma(p_j)$ is the jth column of CRT_m. Since $\vec{d}$ is the dual of $\tau(\vec{p})$, which embeds as $\sigma(\tau(\vec{p})) = \overline{CRT_m}$, we have $\sigma(\vec{d}^T) = (CRT_m^*)^{-1}$.

Remark 9.0.3. If $\mathcal{L} = \mathcal{L}(\mathbb{B})$, then $\mathcal{L}^\vee = \mathcal{L}(\mathbb{B}^{-T})$.

Corollary 9.0.4. The spectral norm of $\vec{d}$ is $s_1(\vec{d}) = \sqrt{\mathrm{rad}(m)/m}$.

Remark 9.0.5. $s_1(\vec{d})$ can be as large as 1, which, unlike $\vec{p}$, is much larger than

$$(\det R^\vee)^{\frac{1}{n}} = \Delta_K^{-\frac{1}{2n}} \approx \frac{1}{\sqrt{n}},$$

which may be thought as the average length of a good basis. The decoding basis is still good choice for discretizing a continuous ring-LWE error, because the input error distribution needs to have Gaussian parameter of at least $\omega(\sqrt{\log n})(\gg 1)$ for provable worst-case hardness. If $\vec{d}$ were defined as the dual of the power basis $\{1, \zeta_m, \cdots, \zeta_m^{\varphi(m)-1}\}$, then the spectral norm of $\vec{d}$ could be much larger: e.g., for $m = 1155 = 3 \cdot 5 \cdot 7 \cdot 11$, $s_1(\vec{d}) \approx 22.6$.

9.1 Relation to the Powerful Basis

Recall that both $\vec{d}$ and $t^{-1}\vec{p}$ are $\mathbb{Z}$-bases of $R^\vee$. We have the following relation between them.

Lemma 9.1.1. Let m be a power of a prime p, and let $m' = m/p$, so that $\varphi(m) = \varphi(p)m'$. Then

$$\vec{d}^T = t^{-1}\vec{p}^T(L_p \otimes I_{[m']}), \tag{9.2}$$

where $L_p \in \mathbb{Z}^{[\varphi(p)]\times[\varphi(p)]}$ is the lower triangular matrix with 1s throughout its lower-left triangle, i.e., its (i,j) entry is 1 for $i \geq j$, and 0 otherwise.

Proof. First reindex the conjugate power basis using the index set $[\varphi(p)] \times [m']$, as

$$\tau(p_{(j_0,j_1)}) = \zeta_p^{-j_0}\zeta_m^{-j_1}.$$

We have to show that

$$\begin{aligned} d_{(j_0,j_1)} &= t^{-1}(\zeta_p^{j_0} + \zeta_p^{j_0+1} + \cdots + \zeta_p^{p-2})\zeta_m^{j_1} & (9.3)\\ &= \frac{1-\zeta_p}{m} \cdot \frac{\zeta_p^{j_0} - \zeta_p^{p-1}}{1-\zeta_p} \cdot \zeta_m^{j_1}, & (9.4)\end{aligned}$$

i.e., the trace of the product of the right hand side with $\tau(p_{(j_0',j_1')})$ is 1 if and only if $(j_0', j_1') = (j_0, j_1)$. We compute the trace of

$$\frac{1}{m}(\zeta_p^{j_0-j_0'} - \zeta_p^{p-1-j_0'})\zeta_m^{j_1-j_1'}. \tag{9.5}$$

From an earlier computation of $\mathrm{Tr}(\zeta_m^j)$, the trace of this is 0 if $j_1 \neq j_1'$ (because $j_1 - j_1' \neq 0 \mod m'$), and 0 if $j_0 \neq j_0'$ (because $j_0 - j_0', p-1-j_0' \neq 0 \mod p$. Note that $j_0, j_0' = 0, 1, \cdots, p-2$.), and otherwise it is $\frac{1}{m}(\varphi(p)m' - (-m')) = \frac{1}{m}(\varphi(p)+1)m' = 1$. ☐

9.2 Decoding $R^\vee$ and its Powers

Recall the decoding procedure: if Λ is a known fixed lattice and $x \in H$ is an unknown short vector, the goal is to recover x, given $t = x \mod \Lambda$. Choose $\{v_i\} \subset \Lambda^\vee$ a set of n-linearly independent vectors, not necessarily a basis, which are rather short and let $\{b_i\}$ be a dual basis of $\{v_i\}$, which generates a super lattice Λ' containing Λ.

Express $t \mod \Lambda'$ in the basis $\{b_i\}$ as $\sum c_i b_i$, $c_i \in \mathbb{R}/\mathbb{Z}$ (so $c_i = \langle x, \bar{v}_i\rangle \mod 1$), then output $\sum [\![c_i]\!] b_i \in H$. Then the output equals x if and only if all the coefficients $a_i = \langle x, \bar{v}_i\rangle$ in the expansion $x = \sum a_i b_i$ are in $[-1/2, 1/2)$. Since $(R^\vee)^\vee = R$ and every p_j of powerful basis of R has $\|\tau(p_j)\|_2 = \sqrt{n}$, we could use the decoding basis $\vec{d}$ for decoding $R^\vee$ because the dual of $\vec{d}$ is $\vec{p}$ and p_j is rather short. But for decoding K/I, where $I = (R^\vee)^k = \langle t^{-k}\rangle$, if we use the $\mathbb{Z}$-basis $t^{1-k}\vec{d}$ of I, some elements of the dual of $(t^{1-k}\vec{d})$, which is $t^{k-1}\tau(\vec{p})$, might be much longer than the shortest nonzero elements of $I^\vee = \langle t^{k-1}\rangle$. (Remark: Let $t = \frac{m}{g}$, where m prime, and $\sigma(g) = (1-\omega_m^1, 1-\omega_m^2, \ldots, 1-\omega_m^{m-2})$. $1-\omega_m$ is very small when m is large. Hence, t is very large.) Instead, we use $\hat{m}^{1-k}\vec{d}$, which generates the super ideal $\mathcal{J} = \hat{m}^{1-k}R^\vee = t^{1-k}g^{1-k}R^\vee \supseteq I$, whose dual elements are $\hat{m}^{k-1}\tau(p) \subset I^\vee$. Note that

$$\frac{\|\hat{m}^{k-1}\tau(\vec{p})\|_2}{\lambda_1(I^\vee)} = \frac{\hat{m}^{k-1}\sqrt{n}}{\lambda_1(I^\vee)} < (\prod_{\text{odd prime } p|m} p^{\frac{1}{p-1}})^{k-1}. \tag{9.6}$$

The last inequality follows from

$$\lambda_1(I^\vee) \geq \sqrt{n}N(R^\vee)^{(1-k)/n} = \sqrt{n}\Delta_K^{(k-1)/n}. \tag{9.7}$$

Decoding I_q to I, where $I = (R^\vee)^k$ for some $k \geq 1$

For an input $\bar{a} \in I_q$, write $\bar{a} = \left\langle \hat{m}^{1-k}\vec{d}, \bar{\mathbf{a}} \right\rangle \mod q\mathcal{J}$ for some $\bar{\mathbf{a}}$ over $\mathbb{Z}_q$, where $\mathcal{J} = \hat{m}^{1-k}R^\vee \supset I$. Define $[\![\bar{a}]\!] := \left\langle \hat{m}^{1-k}\vec{d}, [\![\bar{\mathbf{a}}]\!] \right\rangle$ if this is in I, otherwise the decoding fails. Note if $a \in I$, $a = \left\langle \hat{m}^{1-k}\vec{d}, \mathbf{a} \right\rangle$, and $a_j \in [-q/2, q/2)$, where a_j is jth component of $\mathbf{a}$, then the decoding succeeds. Hence, if every a_j is δ-subgaussian with parameter s, then by lemma 5.2.1, $[\![a \mod qI]\!] = a$ except with probability at most $2n\exp(\delta - \pi q^2/(2s)^2)$.

Writing $a = \left\langle \hat{m}^{1-k}\vec{d}, \mathbf{a} \right\rangle$ for $a \in I$ with integral vector $\mathbf{a}$, we have $|a_j| \leq \hat{m}^{k-1}\sqrt{n}\|a\|_2$, because $|a_j| = |\mathrm{Tr}(a\hat{m}^{k-1}\tau(p_j))| \leq \|a\|_2\hat{m}^{k-1}\sqrt{n}$ by Schwarz inequality.

If a is δ-subgaussian with parameter s and $b \in (R^\vee)^l$ for some $l \geq 0$, we write $ab = \left\langle \hat{m}^{1-k-l}\vec{d}, c \right\rangle$ for some integral vector c. Then

$$
\begin{aligned}
c_j &= \mathrm{Tr}(\hat{m}^{k+l-1}\tau(p_j)ab) && (9.8)\\
&= \hat{m}^{k+l-1}\mathrm{Tr}(\tau(p_j)ba), && (9.9)
\end{aligned}
$$

which is δ-subgaussian with parameter

$$\hat{m}^{k+l-1}\|\tau(p_j)b\|_2 s \leq \hat{m}^{k+l-1}\|\tau(p_j)\|_\infty\|b\|_2 s = \hat{m}^{k+l-1}\|b\|_2 s. \quad (9.10)$$

9.2.1 Implementation of Decoding Operation

The goal is to recover an unknown element $a \in I = (R^\vee)^k$ given $\bar{a} = a \mod qI$. We assume that the input $\bar{a} \in I_q$ is given in the form of a coefficient vector $\bar{\mathbf{a}}$ over $\mathbb{Z}_q$ satisfying $\bar{a} = \left\langle t^{1-k}\vec{b}, \bar{\mathbf{a}} \right\rangle \mod qI$, where $\vec{b}$ is some given $\mathbb{Z}_q$-basis of $R_q^\vee$. Output will be given as a coefficient vector $\mathbf{a}$ over $\mathbb{Z}$ with respect to the decoding basis $t^{1-k}\vec{d}$ of I.

Case 1) $k = 1$.
If $\bar{a} = \left\langle \vec{d}, \bar{\mathbf{a}} \right\rangle \mod qR^\vee$, output $a = \left\langle \vec{d}, \mathbf{a} \right\rangle$ where $\mathbf{a} = [\![\bar{\mathbf{a}}]\!]$.

Case 2) $I = (R^\vee)^k$, $k > 1$.

1. Compute the representation $\bar{a'} = \bar{a} \mod q\mathcal{J}$ in the $\mathbb{Z}_q$-basis $\hat{m}^{1-k}\vec{b}$ of $\mathcal{J}_q$ (recall that $\mathcal{J} = \hat{m}^{1-k}R^\vee \supseteq I$).
2. Decode it as in the case $k = 1$ to an element $a' \in \mathcal{J}$ (which will be equal to a if successful).
3. Compute the representation of a' in the Z-basis $t^{1-k}\vec{d}$ of I.

For *step 1*, we want to find $\bar{\mathbf{a}}$ such that

$$\bar{a} = \left\langle \hat{m}^{1-k}\vec{b}, \bar{\mathbf{a}} \right\rangle \mod q\mathcal{J}. \quad (9.11)$$

We claim that this $\bar{\mathbf{a}}$ is the coefficient of $g^{k-1}\bar{a}$ with respect to the basis $t^{1-k}\vec{b} \mod qI$, because $\left\langle t^{1-k}\vec{b}, \bar{\mathbf{a}} \right\rangle = g^{k-1}\left\langle \hat{m}^{1-k}\vec{b}, \bar{\mathbf{a}} \right\rangle = g^{k-1}\bar{a}$.

For *step 2*, rewrite the output of *step 1* with respect to the basis $\hat{m}^{1-k}\vec{d}$ so that $\bar{a'} = \left\langle \hat{m}^{1-k}\vec{d}, \bar{\mathbf{a}}' \right\rangle$. Then output $[\![\bar{\mathbf{a}}']\!]$ over $\mathbb{Z}$ and let $a' = \left\langle \hat{m}^{1-k}\vec{d}, [\![\mathbf{a}']\!] \right\rangle \in \mathcal{J}$. If it is in I, we succeed. If not, we fail. (Remark: In general, it is easy to decide the membership of a given lattice.)

For *step 3*, we convert the representation of a' in the $\mathbb{Z}$-basis $\hat{m}^{1-k}\vec{d}$ of $\mathcal{J}$ to a representation in a $\mathbb{Z}$-basis of I, namely $t^{1-k}\vec{d}$. Assuming *step 2* succeeds, i.e., $a' \in I$, we want to find an integer vector $\mathbf{a}$ such that $a' = \left\langle t^{1-k}\vec{d}, \mathbf{a} \right\rangle$. For the same $\mathbf{a}$,

$$\left\langle \hat{m}^{1-k}\vec{d}, \mathbf{a} \right\rangle = g^{1-k} \left\langle t^{1-k}\vec{d}, \mathbf{a} \right\rangle = g^{1-k}a',$$

i.e., $\mathbf{a}$ is the coefficient of $g^{1-k}a'$ in the basis $\hat{m}^{1-k}\vec{d}$.

Note that the multiplication by g and the division by g can be computed efficiently. For example when $m = p$,

$$\begin{aligned}
m\vec{d}^T &= (\cdots, (\zeta_p^{j_0} - \zeta_p^{p-1}), \cdots), \quad j_0 = 0, \cdots, p-2, && (9.12)\\
mg\vec{d}^T &= (2 - \zeta_p - \zeta_p^{p-1}, 1 + \zeta_p - \zeta_p^2 - \zeta_p^{p-1}, \cdots, \\
&\quad\; 1 + \zeta_p^{p-2} - \zeta_p^{p-1} - \zeta_p^{p-1}), && (9.13)\\
m\vec{d}^T A &= (1 - \zeta_p^{p-1}, \zeta_p - \zeta_p^{p-1}, \cdots, \zeta_p^{p-2} - \zeta_p^{p-1}) \\
&\quad \times \begin{pmatrix} 2 & 1 & 1 & \cdots & 1 \\ -1 & 1 & & & \\ & -1 & 1 & & \\ & & & \ddots & \\ & & & -1 & 1 \end{pmatrix} && (9.14)\\
&= (2 - \zeta_p - \zeta_p^{p-1}, \cdots), && (9.15)
\end{aligned}$$

i.e., $g\vec{d}^T = \vec{d}^T A$.

9.3 Gaussian sampling in the Decoding Basis

Gaussian sampling a, to be precise $\sigma(a)$, from $K_{\mathbb{R}}$ and representing it with respect the decoding basis can be achieved from the fact that if $a = \left\langle \vec{d}, \mathbf{a} \right\rangle$, then $\mathbf{a} = CRT_m^* \sigma(a)$. Since $CRT_{m_l}^* = (CRT_{p_l}^* \otimes I_{[m_l']})\sqrt{m_l'}Q_l$ for some unitary Q_l,

$$CRT_m^* = \bigotimes_l (CRT_{p_l}^* \otimes I_{[m_l']})\sqrt{m/\operatorname{rad}(m)} \bigotimes_l Q_l. \tag{9.16}$$

Since a spherical Gaussian distribution over $H \subset \mathbb{C}^{\mathbb{Z}_m^*}$ is changed into a spherical Gaussian over $H' = QH \subset \mathbb{C}^{\mathbb{Z}_m^*}$ under the unitary transform Q, it suffices to generate a Gaussian of parameter $s\sqrt{m/\operatorname{rad}(m)}$ over H' and then left multiply the result by

$$C^* := \bigotimes_l CRT_{p_l}^* \otimes I_{[m_l']} = CRT_{\operatorname{rad}(m)}^* \otimes I_{[m/\operatorname{rad}(m)]}. \tag{9.17}$$

Since CRT_m^* sends the elements in H to the real vector space of coefficient vectors with respect to the decoding basis $\vec{d}$, $H' \subset \mathbb{C}^{\mathbb{Z}_m^*}$ can be characterized as follows

$$H' = \{x \in \mathbb{C}^{\mathbb{Z}_m^*} : C^* x \in \mathbb{R}^{[\varphi(m)]}\}. \tag{9.18}$$

For the Gaussian sampling, we have to find a unitary matrix B' made up of the elements of H' such that C^*B' is real. Such B' is given in the form $B'_{p_l} \otimes I_m$, since $C^* = CRT^*_{p_l} \otimes I_{[m_l]}$. We show that

$$B'_{p_l} = \frac{1}{\sqrt{2}} \begin{pmatrix} I & \sqrt{-1}J \\ J & -\sqrt{-1}I \end{pmatrix} \tag{9.19}$$

is one. We check that

$$\begin{aligned} (C^*B') &= (CRT^*_{p_l} B'_{p_l})_{ij} && (9.20)\\ &= (e^{-2\pi i(ji)/p} + e^{-2\pi i(j(p-i))/p})\frac{1}{\sqrt{2}} && (9.21)\\ &= \frac{1}{\sqrt{2}}(e^{-2\pi i(ji)/p} + e^{2\pi i(ji)/p}) \in \mathbb{R}. && (9.22) \end{aligned}$$

Note that

$$CRT^*_p = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ & & & \\ & & \omega_p^{-(ij)} & \\ & & & \end{pmatrix}. \tag{9.23}$$

Our $B' = B'_{p_l} \otimes I_m$ is different from previous basis of H,

$$B = \frac{1}{\sqrt{2}} \begin{pmatrix} I & \sqrt{-1}J \\ J & -\sqrt{-1}I \end{pmatrix} \in \mathbb{C}^{\mathbb{Z}^*_m \times [\varphi(m)]}. \tag{9.24}$$

Even though the B'_{p_l} part looks the same, B' is a basis of H', not H.

Remark 9.3.1. The final vector of the decoding basis coefficients is $C^*B'\mathbf{c}$ for a real Gaussian $\mathbf{c}$.

Chapter 10

Regularity

Let $R = \mathbb{Z}[\zeta_m]$, $n = \varphi(m)$, and $q \geq 1$ a prime. Let $a_1, \ldots, a_{l-1}$ be chosen uniformly and independently from R_q (l could be small). Then we claim that with high probability over the choice of a_i, the distribution of $b_0 + \sum_{i=1}^{l-1} b_i a_i$ is within the statistical distance $2^{-\Omega(n)}$ of uniform, where b_i are chosen from a discrete Gaussian distribution on R of width essentially $nq^{1/l}$.

$nq^{1/l}$ is the best possible in some sense, since R is a rotation of $\sqrt{n}\mathbb{Z}^n$, so the discrete Gaussian of width t covers $\left(\frac{t}{\sqrt{n}}\right)^n$ lattice points. $\left(\frac{t}{\sqrt{n}}\right)^l \approx q^n$ implies $t \sim \sqrt{n}q^{1/l}$.

If we consider the more general combination $\sum_{i=0}^{l-1} b_i a_i$, then the regularity lemma fails if l is small. For example, when q is a prime satisfying $q = 1 \mod m$, so that $\langle q \rangle$ splits completely into n ideals of norm q each. Let $\mathfrak{q}$ denote one of these prime factors. With probability q^{-l} all a_i are in $\mathfrak{q}$, so in this case $\sum_{i=1}^{m} b_i a_i$ is in $\mathfrak{q}$ with certainty whose distribution is very far from uniformity. By adding the b_0 term, we avoid this common divisor problem.

Lemma 10.0.2. For any n-dimensional lattice Λ and ε, $r > 0$,

$$\rho_{1/r}(\Lambda) \leq \max\left(1, \left(\frac{\eta_\varepsilon(\Lambda^\vee)}{r}\right)^n\right)(1+\varepsilon). \tag{10.1}$$

Proof. For $r \geq \eta_\varepsilon(\Lambda^\vee)$, the claim follows from the definition of smoothing parameter $\eta_\varepsilon(\Lambda^\vee)$. For $r < \eta = \eta_\varepsilon(\Lambda^\vee)$,

$$\begin{aligned} \rho_{1/r}(\Lambda) &= (\det\Lambda)^{-1} r^{-n} \rho_r(\Lambda^\vee) \quad \text{(by Poisson summation formula)} & (10.2)\\ &< (\det\Lambda)^{-1} r^{-n} \rho_\eta(\Lambda^\vee) = \left(\frac{\eta}{r}\right)^n \rho_{1/\eta}(\Lambda). & (10.3) \end{aligned}$$

□

In particular,

$$\rho_{1/r}(I) \leq \max(1, N(I)^{-1} r^{-n})(1 + 2^{-2n}), \tag{10.4}$$

since $\eta_{2^{-2n}}(I^\vee) \leq \sqrt{n}/\lambda_1(I) \leq (N(I))^{-1/n}$.

Lemma 10.0.3. In the mth cyclotomic number field of degree n, for any q, $k \geq 1$,

$$\sum_{\mathcal{J} | \langle q \rangle} N(\mathcal{J})^k \leq \exp(3c) q^{kn} \leq q^{kn+5}, \tag{10.5}$$

where c is the number of distinct prime integer divisors of q.

Proof. Since $c \leq \log_2 q$ and $e^{3c} \leq e^{3\log_2 q} < q^5$, the second inequality is trivial. For the first inequality, we may assume $q = p^e$. Indeed, if q_1 and q_2 are coprime, then

$$\sum_{\mathcal{J}|\langle q_1 q_2\rangle} N(\mathcal{J})^k = \left(\sum_{\mathcal{J}|\langle q_1\rangle} N(\mathcal{J})^k\right)\left(\sum_{\mathcal{J}|\langle q_2\rangle} N(\mathcal{J})^k\right), \tag{10.6}$$

since when q_1 and q_2 are coprime, any $\mathcal{J}|\,\langle q_1q_2\rangle$ is of the form $\mathcal{J} = \mathcal{J}_1\mathcal{J}_2$, where $\mathcal{J}_1|\,\langle q_1\rangle$, $\mathcal{J}_2|\,\langle q_2\rangle$, and $N(\mathcal{J}_1\mathcal{J}_2) = N(\mathcal{J}_1)N(\mathcal{J}_2)$, because the ring of integers R is a UFD. Now $\langle p\rangle = p_1^h \cdots p_g^h$ in R, where $h = \varphi(p^d)$, $d \geq 0$ is the largest integer such that p^d divides m, each p_i is of norm p^f, where $f \geq 1$ is the multiplicative order of p modulo m/p^d, and $g = n/hf$, so we have $\langle q\rangle = p_1^{eh}\cdots p_g^{eh}$, and

$$\begin{aligned}
\sum_{\mathcal{J}|\langle q\rangle} N(\mathcal{J})^k &= \prod_{i=1}^{g}(1 + N(p_i)^k + \cdots + N(p_i)^{ehk}) && (10.7)\\
&= (1 + p^{fk} + \cdots + p^{ehfk})^g && (10.8)\\
&\leq p^{ehfkg}(1 - p^{-fk})^{-g} && (10.9)\\
&\leq q^{nk}\exp(3gp^{-fk}). && (10.10)
\end{aligned}$$

Remark 10.0.4.

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots < e^{3x} = 1 + 3x + \frac{(3x)^2}{2} + \cdots \tag{10.11}$$

when $x < \frac{1}{2}$.

Observe that $p^f > m/p^d$, since $p^f = 1 \mod m/p^d$ and $p^f > 1$.

$$g \leq n/\varphi(p^d) = \varphi(m/p^d) < \frac{m}{p^d},$$

hence $gp^{-fk} \leq gp^{-f} < 1$, which proves

$$\sum_{\mathcal{J}|\langle q\rangle} N(\mathcal{J})^k \leq q^{nk}e^3. \tag{10.12}$$

Hence, for general q, we have

$$\sum_{\mathcal{J}|\langle q\rangle} N(\mathcal{J})^k \leq \exp(3c)q^{kn} \leq q^{kn+5}. \tag{10.13}$$

($\because \exp(3c) < \exp(3\log_2 q) = \exp(\log_2 q^3) < q^5$) $\square$

For a matrix $A \in R_q^{[k]\times[l]}$, we define

$$\Lambda^\perp(A) = \{\vec{z} \in R^{[l]} : A\vec{z} = 0 \mod qR\}. \tag{10.14}$$

Theorem 10.0.5. Let R be the ring of integers in the mth cyclotomic number field K of degree n, and $q \geq 2$ an integer. For positive integers $k \leq l \leq \mathrm{poly}(n)$, let $A = \left[I_{[k]}|\bar{A}\right] \in (R_q)^{[k]\times[l]}$, where $I_{[k]} \in (R_q)^{[k]\times[k]}$ is the identity matrix and $\bar{A} \in R_q^{[k]\times[l-k]}$ uniformly random. Then for all $r > 2n$,

$$\mathbb{E}_{\bar{A}}[\rho_{1/r}(\Lambda^\perp(A)^\vee)] \leq 1 + 2\left(\frac{r}{n}\right)^{-nl} q^{kn+5} + 2^{-\Omega(n)}. \tag{10.15}$$

In particular, if $r > 2nq^{\frac{k}{l}+\frac{5}{nl}}$, then $\mathbb{E}_{\bar{A}}[\rho_{1/r}(\Lambda^\perp(A)^\vee)] \leq 1+2^{-\Omega(n)}$, hence $\eta_{2^{-\Omega(n)}}(\Lambda^\perp(A)) \leq r$ except with probability at most $2^{-\Omega(n)}$.

Corollary 10.0.6. Let R, n, q, k and l as above. Assume $A = [I_{[k]}|\bar{A}] \in (R_q)^{[k]\times[l]}$ is chosen as above. Then with probability $1 - 2^{-\Omega(n)}$ over the choice of $\bar{A}$, the distribution of $A\vec{x} \in R_q^{[k]}$, where each coordinate of $\vec{x} \in R_q^{[l]}$ is chosen from a discrete Gaussian distribution of parameter $r > 2nq^{k/l+5/nl}$ over R, satisfies that the probability of each of the q^{nk} possible outcomes is almost uniform, i.e., is in the interval $(1 \pm 2^{-\Omega})q^{-nk}$.

Proof. Since in this case

$$\eta_{2^{-\Omega(n)}}(\Lambda^{\perp}(A)) \leq r \tag{10.16}$$

except with probability at most $2^{-\Omega(n)}$,

$$\rho_r(\Lambda^{\perp}(A) + c) \in [1 \pm 2^{-\Omega(n)}]r^n \det(\Lambda)^{-1}, \tag{10.17}$$

i.e., $\forall c \in R_q^{[k]}$. Hence, every $c \in R_q^{[k]}$ occurs almost uniformly, since the probability of $A\vec{x} = c$ is proportional to $\rho(\Lambda^{\perp}(A) + c)$. $\square$

Proof of Theorem. Since $x \in \Lambda^{\perp}(A) \Leftrightarrow Ax = 0 \mod qR^{[k]}, x \in R^{[l]}$, and $y \in \Lambda^{\perp}(A)^{\vee}$, i.e., $\langle y, x\rangle \in \mathbb{Z}\ \forall x \in \Lambda^{\perp}(A)$, it is easy to see that

$$(R^{\vee})^{[l]} + \left\{\tfrac{1}{q}A^T\vec{s} : \vec{s} \in (R_q^{\vee})^{[k]}\right\} \subset \Lambda^{\perp}(A)^{\vee}. \tag{10.18}$$

(For example, $\left\langle \frac{1}{q}A^T\vec{s}, x\right\rangle = \frac{1}{q}\langle \vec{s}, Ax\rangle \in \mathbb{Z}$ since $Ax \in qR^{[k]}$.) To show the other inclusion relation, we consider the simple case, when

$$A \in \mathbb{Z}_q^{n\times m}, \quad \Lambda^{\perp}(A) = \{y \in \mathbb{Z}^m : Ay = 0 \mod q\}. \tag{10.19}$$

Then

$$\Lambda^{\perp}(A)^{\vee} \supset \mathbb{Z}^m + \left\{\tfrac{1}{q}A^Ts : s \in \mathbb{Z}_q^n\right\}. \tag{10.20}$$

We assume that $A : \mathbb{Z}_q^m \to \mathbb{Z}_q^n$ is onto as in our case. Then $\det(\Lambda^{\perp}(A)) = q^n$, which is the number of cosets. To show $\Lambda^{\perp}(A)^{\vee} = \mathbb{Z}^m + \left\{\frac{1}{q}A^Ts : s \in \mathbb{Z}_q^n\right\}$, it suffices to show that the determinant of RHS is $\frac{1}{q^n}$. To prove this, assume two translates of $\mathbb{Z}^m$,

$$\mathbb{Z}^m + \tfrac{1}{q}A^Ts = \mathbb{Z}^m + \tfrac{1}{q}A^Ts', \quad s, s' \in \mathbb{Z}_q^n. \tag{10.21}$$

Then $\frac{1}{q}A^T(s - s') \in \mathbb{Z}^m$, so $A^T(s - s') = 0 \mod q$. Hence, $s - s' = 0 \mod q$ because $\operatorname{rank}(A) = n$. That is, the determinant of RHS is $\frac{1}{q^n}$ because RHS is the union of q^n different translates of $\mathbb{Z}^m$. The proof for the general case of Λ is the same.

Now we compute

$$\mathbb{E}_A[\rho_{1/r}(\Lambda^{\perp}(A)^{\vee})] = \sum_{\vec{s}\in(R_q^{\vee})^{[k]}} \mathbb{E}_A\left[\rho_{1/r}\left((R^{\vee})^l + \tfrac{1}{q}A^T\vec{s}\right)\right] \tag{10.22}$$

$$= \left(\sum_{\vec{s}\in(R_q^{\vee})^{[k]}} \rho_{1/r}\left((R^{\vee})^{[k]} + \tfrac{1}{q}\vec{s}\right)\right) \mathbb{E}_{\vec{a}}\left[\rho_{1/r}\left(R^{\vee} + \tfrac{1}{q}\langle\vec{a}, \vec{s}\rangle\right)\right]^{l-k}, \tag{10.23}$$

where $\vec{a}$ represents a typical column vector of $\bar{A}$, since $\|x\|^2 = \|x_1\|^2 + \|x_2\|^2$ for $x = (x_1, x_2) \in (R^{\vee})^{[k]} \times (R^{\vee})^{[l-k]}$, and

$$\rho_{1/r}(x) = e^{-\pi r\|x\|^2} = e^{-\pi r\|x_1\|^2} \cdot e^{-\pi r\|x_2\|^2}, e^{-\pi r\|y\|^2} = e^{-\pi r y_1^2} \cdots e^{-\pi r y_n^2}. \tag{10.24}$$

In Eq. (10.22), note that $\frac{1}{q}A^T\vec{s} \neq \frac{1}{q}A^T\vec{s'}$ if $\vec{s} \neq \vec{s'}$ in $(R_q^\vee)^{[k]}$, since A is onto, hence A^T is injective.

For any given $\vec{s} = (s_1, \ldots, s_k) \in (R_q^\vee)^{[k]}$, define the ideal

$$I_{\vec{s}} = s_1R + \cdots + s_kR + qR^\vee \subseteq R^\vee.$$

Then $(R_q)^{[k]} \ni \vec{a} \to \langle \vec{a}, \vec{s} \rangle$ uniformly random over $I_{\vec{s}}/qR^\vee$, since $\vec{a}$, which is a column of $\bar{A}$, is uniformly random. Since $\displaystyle\bigsqcup_{\vec{a}\in I_{\vec{s}}/qR^\vee} R^\vee + \frac{1}{q}\langle \vec{a}, \vec{s} \rangle = \frac{1}{q}I_{\vec{s}}$,

$$\sum_{\vec{a}\in I_{\vec{s}}/qR^\vee} \rho_{\frac{1}{r}}\left(R^\vee + \frac{1}{q}\langle \vec{a}, \vec{s} \rangle\right) = \rho_{\frac{1}{r}}\left(\frac{1}{q}I_{\vec{s}}\right), \tag{10.25}$$

where $\vec{a}$ is a representative of a different coset element of $I_{\vec{s}}/qR^\vee$. Hence,

$$\mathbb{E}_{\vec{a}}\left[\rho_{1/r}\left(R^\vee + \tfrac{1}{q}\langle \vec{a}, \vec{s} \rangle\right)\right] = \frac{\rho_{1/r}\left(\frac{1}{q}I_{\vec{s}}\right)}{|I_{\vec{s}}/qR^\vee|}. \tag{10.26}$$

Note that when $x \in \{1, \cdots, n\}$ is uniformly chosen,

$$\mathbb{E}_x f(x) = \frac{f(x_1) + \cdots + f(x_n)}{n} = \frac{f(x_1 \cup \cdots \cup x_n)}{n}, \tag{10.27}$$

where $f(A) = \sum_{x\in A} f(x)$.
Let T denote the set of all ideals $\mathcal{J}$ satisfying $qR^\vee \subseteq \mathcal{J} \subseteq R^\vee$. Then we can write Eq. (10.23) as

$$\begin{aligned}
&\left(\sum_{\mathcal{J}\in T} |\mathcal{J}/qR^\vee|^{-(l-k)} \cdot \rho_{1/r}\left(\tfrac{1}{q}\mathcal{J}\right)^{l-k}\right) \cdot \left(\sum_{\vec{s}\text{ s.t.} I_{\vec{s}}=\mathcal{J}} \rho_{1/r}\left((R^\vee)^{[k]} + \tfrac{1}{q}\vec{s}\right)\right) \\
&\quad \leq \rho_{\frac{1}{r}}(R^\vee)^l_{(s=0)} + \sum_{\mathcal{J}\in T\setminus\{qR^\vee\}} |\mathcal{J}/qR^\vee|^{-(l-k)} \cdot \rho_{\frac{1}{r}}\left(\tfrac{1}{q}\mathcal{J}\right)^{l-k} \cdot \left(\rho_{\frac{1}{r}}\left(\tfrac{1}{q}\mathcal{J}\right)^k - 1\right).
\end{aligned} \tag{10.28}$$

Now Eq. (10.28) satisfies

$$\begin{aligned}
&\rho_{\frac{1}{r}}(R^\vee)^l + \sum_{\mathcal{J}\in T\setminus\{qR^\vee\}} |\mathcal{J}/qR^\vee|^{-(l-k)} \cdot \rho_{\frac{1}{r}}\left(\tfrac{1}{q}\mathcal{J}\right)^{l-k} \cdot \left(\rho_{\frac{1}{r}}\left(\tfrac{1}{q}\mathcal{J}\right)^k - 1\right) && (10.29)\\
&\leq \rho_{\frac{1}{r}}(R^\vee)^l + \sum_{\mathcal{J}\in T\setminus\{qR^\vee\}} |\mathcal{J}/qR^\vee|^{-(l-k)} \cdot \left(\rho_{\frac{1}{r}}\left(\tfrac{1}{q}\mathcal{J}\right)^l - 1\right) && (10.30)\\
&= 1 + \sum_{\mathcal{J}\in T} |\mathcal{J}/qR^\vee|^{-(l-k)} \left(\rho_{\frac{1}{r}}\left(\tfrac{1}{q}\mathcal{J}\right)^l - 1\right), && (10.31)
\end{aligned}$$

so

$$\begin{aligned}
\rho_{\frac{1}{r}}(\tfrac{1}{q}\mathcal{J})^l &\leq \max(1, (|\mathcal{J}/qR^\vee|\Delta_K r^{-n})^l) \times (1 + 2^{-2n})^l && (10.32)\\
&\leq 1 + l2^{1-2n} + 2(|\mathcal{J}/qR^\vee|\Delta_K r^{-n})^l, && (10.33)
\end{aligned}$$

where (10.32) follows from

$$\eta_{2^{-2n}}\left(\left(\frac{\mathcal{J}}{q}\right)^{\vee}\right) \leq \frac{\sqrt{n}}{\lambda_1\left(\left(\frac{\mathcal{J}}{q}\right)^{\vee}\right)} \leq \left(N\left(\frac{\mathcal{J}}{q}\right)\right)^{-1/n}$$

and

$$N\left(\frac{\mathcal{J}}{q}\right)^{-1} = \left|\frac{\mathcal{J}}{qR}\right| = \left|\frac{R^{\vee}}{R}\right| \cdot \left|\frac{\mathcal{J}}{q}\Big/R^{\vee}\right| = \Delta_K|\mathcal{J}/qR^{\vee}|.$$

Hence,

$$\begin{aligned}(10.31) &< 1 + 2^{-\Omega(n)} + 2\Delta_K^l r^{-nl}\sum_{\mathcal{J}\in T}\left|\frac{\mathcal{J}}{qR^{\vee}}\right|^k && (10.34)\\ &\leq 1 + 2^{-\Omega(n)} + 2(r/n)^{-nl}q^{kn+5}, && (10.35)\end{aligned}$$

since $\Delta_K \leq n^n$ and

$$\sum_{\mathcal{J}\in T}|\mathcal{J}/qR^{\vee}|^k = \sum_{\mathcal{J}|\langle q\rangle} N(\mathcal{J})^k \leq q^{kn+5}. \tag{10.36}$$

Note that $|\frac{\mathcal{J}}{qR^{\vee}}| = |\frac{R}{q\mathcal{J}^{\vee}}|$ and $q\mathcal{J}^{\vee} \supset qR$.

$$\begin{aligned}&qR^{\vee} \subset \mathcal{J} \subset R^{\vee} && (10.37)\\ &\tfrac{1}{q}R \supset \mathcal{J}^{\vee} \supset R && (10.38)\\ &R \supset q\mathcal{J}^{\vee} \supset qR && (10.39)\end{aligned}$$

Conversely,

$$\begin{aligned}&R \supset I \supset qR && (10.40)\\ &R^{\vee} \subset I^{\vee} \subset \tfrac{1}{q}R^{\vee} && (10.41)\\ &qR^{\vee} \subset qI^{\vee} \subset R^{\vee} && (10.42)\end{aligned}$$

i.e., there is a bijective correspondence

$$\{\text{ideal } \mathcal{J} : qR^{\vee} \subset \mathcal{J} \subset R^{\vee}\} \longleftrightarrow \{\text{ideal } I : R \supset I \supset qR\}.$$

□

Remark 10.0.7. If $qR \subsetneq \mathcal{J}$, then

$$\sum_{\vec{s}\text{ s.t.}I_{\vec{s}}=\mathcal{J}} (R^{\vee})^{[k]} + \tfrac{1}{q}\vec{s} \subseteq (\tfrac{1}{q}\mathcal{J})^{[k]} \setminus 0, \text{ since } \vec{s} \neq 0. \tag{10.43}$$

Hence,

$$\begin{aligned}\sum_{\vec{s}\text{ s.t.}I_{\vec{s}}=\mathcal{J}} \rho_{\frac{1}{q}}\left((R^{\vee})^k + \frac{1}{q}\vec{s}\right) &\subset \rho_{\frac{1}{r}}\left(\left(\frac{1}{q}\mathcal{J}\right)^{[k]}\right) - 1 && (10.44)\\ &= \rho_{\frac{1}{r}}\left(\frac{1}{q}\mathcal{J}\right)^k - 1. && (10.45)\end{aligned}$$

Remark 10.0.8. Another computation:

$$\rho_{\frac{1}{r}}\Big((R^\vee)^{[k]} + \tfrac{1}{q}\vec{s}\Big) = \prod_{i=1}^{k} \rho_{\frac{1}{r}}(R^\vee + \tfrac{1}{q}s_i) \tag{10.46}$$

$$\leq \rho_{\frac{1}{r}}(\tfrac{1}{q}\mathcal{J})^{k-1} \cdot \Big(\rho_{\frac{1}{r}}(\tfrac{1}{q}\mathcal{J}) - 1\Big) \tag{10.47}$$

$$\leq \rho_{\frac{1}{r}}(\tfrac{1}{q}\mathcal{J})^{k} - 1, \tag{10.48}$$

where (10.47) follows since $s_i \neq 0$ for some i and $R^\vee + \frac{1}{q}s_i \subset \frac{1}{q}\mathcal{J}$, and (10.48) follows from $\rho_{\frac{1}{r}}(\frac{1}{q}\mathcal{J}) > 1$.

Chapter 11

Cryptosystems

(q should be larger than p, but the smaller the better for the efficiency)

11.1 Dual-Style Cryptosystem [GPV08]

- Gen: choose $a_0 = -1 \in R_q$, uniformly random and independent $a_1, \dots, a_{l-1} \in R_q$, and independent $x_0, \dots, x_{l-1} \leftarrow D_{R,r}$. Output

$$\vec{a} = (a_1, \dots, a_{l-1}, a_l = -\sum_{i \in [l]} a_i x_i) \in R_q^{\{1,2,\dots,l\}}$$

as the public key, and

$$\vec{x} = (x_1, \dots, x_{l-1}, x_l = 1) \in R^{\{1,2,\dots,l\}}$$

as the secret key. Note that $\langle \vec{a}, \vec{x} \rangle = x_0 \in R_q$.

- $\mathrm{Enc}_{\vec{a}}(\mu \in R_p)$: choose independent $e_0, e_1, \dots, e_{l-1} \leftarrow \lfloor p\psi \rceil_{pR^\vee}$ and $e_l \leftarrow \lfloor p\psi \rceil_{t^{-1}\mu + pR^\vee}$ (shifted error). Let $\vec{e} = (e_1, \dots, e_l) \in (R^\vee)^{\{1,\dots,l\}}$. Output the ciphertext

$$\vec{c} = e_0 \vec{a} + \vec{e} \in (R_q^\vee)^{\{1,\dots,l\}},$$

l-samples of Ring-LWE.

- $\mathrm{Dec}_{\vec{x}}(\vec{c})$: compute $d = [\![\langle \vec{c}, \vec{x} \rangle]\!] \in R^\vee$ and output $\mu = td \mod pR$.

If $r > 2n \cdot q^{1/l + 2/nl}$, then $(a_1, a_2, \dots, a_l)$ approximating uniform and the above cryptosystem is secure under the hardness R-LWE because ciphertext $\vec{c} = e_0 \vec{a} + \vec{e}$ is a Ring-LWE with proper security.

Theorem 11.1.1. Suppose that for any $c \in R_q^\vee$, $\lfloor p\psi \rceil_{c+pR^\vee}$ is δ-subgaussian with parameter s for some $\delta = \mathcal{O}(\frac{1}{l})$, and $q \geq s\sqrt{(r^2 l + 1)n} \cdot \omega(\sqrt{\log n})$. Then the decryption is correct with probability $1 - negl(n)$ over all the randomness of key generation and encryption.

Remark 11.1.2. If ψ is continuous Gaussian with parameter $s' > 1$ and if we use coordinate-wise randomized rounding, then since $s_1(\vec{d}) = \sqrt{\frac{\mathrm{rad}(m)}{m}}$ and the sum of two independent Gaussians is again Gaussian with the sum of variances as the new variance, $\lfloor p\psi \rceil_{c+pR^\vee}$ is 0-subgaussian with parameter $s = p\sqrt{s'^2 + 2\pi\,\mathrm{rad}(m)/m} = \mathcal{O}(ps')$.

($2\pi\frac{\mathrm{rad}(m)}{m}$ comes from discretization by coordinate-wise randomized rounding and multiplication by $\vec{d}$, since if $\mathbb{E}(X) = 0$ and $|X| \leq B$, then X is 0-subgaussian with parameter $B\sqrt{2\pi}$.)

Proof. By construction, $\langle \vec{c}, \vec{x} \rangle = e_0 z_0 + \langle \vec{e}, \vec{x} \rangle = \left\langle \vec{e'}, \vec{x'} \right\rangle \mod qR^\vee$, where $\vec{e'} = (e_0, e_1, \ldots, e_l)$, $\vec{x'} = (x_0, x_1, \ldots, x_l = 1)$, and $\left\langle \vec{e'}, \vec{x'} \right\rangle = t^{-1}\mu \mod pR^\vee$, so decryption is correct as long as

$$[\![\left\langle \vec{e'}, \vec{x'} \right\rangle \mod qR^\vee]\!] = \left\langle \vec{e'}, \vec{x'} \right\rangle \in R^\vee. \tag{11.1}$$

With high probability, $\|x_i\|_2 \leq r\sqrt{n}$, $\|x_l\| = \|1\|_2 = \sqrt{n}$. Therefore each coefficient of $e_i x_i$ with respect to decoding basis is δ-subgaussian with parameter $sr\sqrt{n}$, and $e_l x_l$ is δ-subgaussian with parameter $s\sqrt{n}$. Hence, each decoding basis coefficient of $\left\langle \vec{e'}, \vec{x'} \right\rangle$ is $\delta(l+1)$-subgaussian with parameters $s\sqrt{(r^2 l + 1) + n}$. By decoding I_q to I lemma, this proves the theorem. □

11.2 Compact Public-key Cryptosystem

Let $R = \mathbb{Z}[\zeta_m]$, and p, q coprime integers, R_p the message space. q is coprime with every odd prime dividing m.

- *Gen*: choose a uniformly $a \leftarrow R_q$. Choose $x \leftarrow \lfloor \psi \rceil_{R^\vee}$ and $e \leftarrow \lfloor p\psi \rceil_{pR^\vee}$. Output $(a, b = \hat{m}(ax + e) \mod qR) \in R_q \times R_q$ as public key, and x as the secret key. (Note that $\hat{m}(ax + e) \in gR/gqR$, even $ax + e \in R^\vee/qR^\vee$, because $\hat{m} = tg$.)
- $Enc_{(a,b)}(\mu \in R_p)$: choose $z \leftarrow \lfloor \psi \rceil_{R^\vee}$, $e' \leftarrow \lfloor p\psi \rceil_{pR^\vee}$ and $e'' \leftarrow \lfloor p\psi \rceil_{t^{-1}\mu + pR^\vee}$. Let $u = \hat{m}(za + e') \mod qR$ and $v = zb + e'' \in R_q^\vee$. Output $(u, v) \in R_q \times R_q^\vee$.
- $Dec_x(u, v)$: compute $v - ux = z\hat{m}(ax + e) + e'' - \hat{m}(za + e')x = \hat{m}(ez - e'x) + e''$ mod $qR^\vee$, decode it to $d = [\![v - ux]\!] \in R^\vee$. Output $\mu = td \mod pR$.

Theorem 11.2.1. The above cryptosystem is secure assuming the hardness of $R-DLWE_{q,\psi}$.

Proof. If $(a, ax + e) \in R_q \times R_q^\vee$ is indistinguishable from uniform, then $(a, \hat{m}(ax + e)) \in R_q \times R_q$ is indistinguishable from uniform, since $\hat{m}R_q^\vee = gR$, and $\langle g \rangle$, $\langle q \rangle$ are coprime. Hence, we may assume that the public key (a, b) is uniformly random in $R_q \times R_q$. We have to prove that $(a, b, Enc_{(a,b)}(\mu))$ is computationally indistinguishable from uniform for any message $\mu \in R_p$. We know that uniform distribution and $A_{z,\psi}($ for $z \leftarrow \lfloor \psi \rceil_{R^\vee})$ over $R_q \times K_{\mathbb{R}}/qR^\vee$ are computationally indistinguishable from LWE assumption. Now do the following process. Choose two samples from either uniform or $A_{z,\psi}$ (which we cannot distinguish). (We may assume that (a, b) is uniform because of R-LWE.) Let them be (a', u'') and (b', v'), and apply the discretization process with $w = 0$ to (a', u'') to obtain (a, u'), and with $w = t^{-1}\mu \in R_p^\vee$ to (b', v') to obtain (b, v). Then output (a, b) as the public key and $(u = \hat{m}u' \mod qR, v) \in R_q \times R_q^\vee$ as the encryption of μ. If we sampled both from uniform, then (a, b, u, v) is uniform in $R_q^{[3]} \times R_q^\vee$. If we sampled both from $A_{z,\psi}$, then (a, b) is uniform and (u, v) has the same distribution as the one generated by $Enc_{(a,b)}(\mu)$. This means that if we can distinguish random (a, b, u, v) and $(a, b, Enc_{a,b}(\mu))$, we can distinguish uniform distribution and $A_{z,\psi}$ over $R_q \times K_{\mathbb{R}}/qR^\vee$, which is a contradiction to the R-LWE assumption. This completes the proof. □

Lemma 11.2.2. Suppose that $\lfloor \psi \rceil_{R^\vee}$ outputs elements having l_2 norm bounded by l with $1-negl(n)$ probability, that $\lfloor p\psi \rceil_{e+pR^\vee}$ is δ-subgaussian with parameters s for some $\delta = \mathcal{O}(1)$, and that $q \geq s\sqrt{2(\hat{m}l)^2 + n}\omega(\sqrt{\log n})$. Then the decryption is correct with probability $1 - negl(n)$ over all the randomness of key generation and encryption.

Proof. e, $e' \in pR^\vee$ and x, $z \in R^\vee$, hence $\hat{m}(e \cdot z - e' \cdot x) \in pR^\vee$, because $\hat{m} = tg$. Therefore $E := \hat{m}(ez - e'x) + e'' \in R^\vee$ satisfies $E = t^{-1}\mu \mod pR^\vee$. So decryption is correct as long as $[\![E \mod qR^\vee]\!] = E$. By assumption, $\|x\|_2$, $\|z\|_2 \leq l$ with probability $1 - negl(n)$, and e, e', e'' are δ-subgaussian with parameter s. Hence, each coefficient of $\hat{m} \cdot ez$, $\hat{m} \cdot e'x \in R^\vee$ when represented in the decoding basis is δ-subgaussian with parameter $s\hat{m}l$ and those of e'' are δ-subgaussian with parameter $s\sqrt{n}$ ($\because b = 1$ in this case, and $\|1\|_2 = \sqrt{n}$). Since e, e', e'' are mutually independent, each decoding basis coefficient of E is 3δ-subgaussian with parameter $s\sqrt{2(\hat{m}l)^2 + n}$. The statement follows from decoding I_q to I lemma. □

11.3 Homomorphic Cryptosystem

- Notations

  R: mth cyclotomic ring of degree $n = \varphi(m)$

  p, q coprime

  R_p: the message space

  q: the Ring-LWE modulus

  $\langle p \rangle$, $\langle g \rangle \subset R$ coprime, i.e., p is coprime with all primes dividing m

- *Gen*: $s' \leftarrow \lfloor \psi \rceil_{R^\vee}$ output $s = ts'$ as secret key.

- $Enc_s(\mu \in R_p)$: $e \leftarrow \lfloor p\psi \rceil_{t^{-1}\mu + pR^\vee}$. Let $c_0 = -c_1 s + e \in R_q^\vee$ for uniformly random $c_1 \leftarrow R_q^\vee$, and output the ciphertext $c(S) = c_0 + c_1 S$, where S is indeterminate. $e(= c(s))$ is called the noise even though from e, we obtain the message μ ($te = \mu \mod pR$).

- $Dec_s(c(S))$ for c of degree k: compute $c(s) \in (R_q^\vee)^k$ and decode it to $e = [\![c(s)]\!] \in R^\vee$. Output $\mu = t^k e \mod pR$.

- Homomorphic product is standard polynomial multiplication $c(S)c'(S)$.

- Homomorphic sum is defined for ciphertexts c, c' of equal degree as $c(S) + c'(S)$.

To homomorphically add two ciphertexts of different degrees, we must first homomorphically multiply the one having smaller degree by a fixed public encryption of $1 \in R_p$ enough times to match the larger degree.

From decoding lemma in $R^\vee$, we obtain the following lemma.

Lemma 11.3.1. If q is large enough, or more precisely if the noise e in a degree k ciphertext c is δ-subgaussian with parameter r for some $\delta = \mathcal{O}(1)$, and $q \geq r\hat{m}^{k-1}\sqrt{n}\omega(\sqrt{\log n})$, then $Dec_s(c)$ correctly recovers e with probability $1-negl(n)$. Moreover if $q > 2\|e\|_2\hat{m}^{k-1}\sqrt{n}$, then $Dec_s(c)$ recovers with certainty.

Lemma 11.3.2. The above cryptosystem is secure assuming the hardness of $R\text{–}DLWE_{q,\psi}$.

Proof. We have access to two distributions over $R_q \times K_{\mathbb{R}}/qR^\vee$, either LWE distribution $A_{s',\psi}$ where $s' \leftarrow \lfloor \psi \rceil_{R^\vee}$ or the uniform distribution. Draw a sample from $(a', b') \in R_q \times K_{\mathbb{R}}/qR^\vee$ from the unknown distribution. Let $a = pa' \mod qR$ and $b = \lfloor pb' \rceil_{t^{-1}\mu + pR^\vee}$ to obtain $(a, b) \in R_q \times R_q^\vee$. Let $c_1 = -t^{-1}a \in R_q$, $c_0 = b$, and output $c(S) = c_0 + c_1 S$. If the unknown distribution is $A_{s',\psi}$, then $c(S)$ is distributed exactly according to $Enc_s(\mu)$. If the unknown distribution is the uniform distribution, then (a, b) is uniform and independent of μ. Hence, $c(S)$ uniform. Therefore, if somebody distinguishes the ciphertext $c(S)$ and the uniform $c(S)$, then he can solve $R - DLWE$, which contradicts the hardness assumption of $R - DLWE$. □

11.3.1 Modulus Reduction and Key Switching

We need large modulus q for the correct $Dec_s(c)$, but for the efficiency, the smaller q is, the better. For this purpose, we describe modulus reduction.

Let $\mathcal{J}$ be a fractional ideal, something like $(R^\vee)^k$, and q, q', p integers with both q and q' coprime to p. Let $v \in \mathbb{Z}_p$ be $v = q'q^{-1} \mod p$. Define a randomized function $F_{\mathcal{J}} : \mathcal{J}_q \to K$ as follows. Assume that a good basis of $\mathcal{J}$ is given and $x \in \mathcal{J}_q$. Then $F_{\mathcal{J}}(x)$ is a short subgaussian element from the coset $(v - q'/q)x + p\mathcal{J}$. Note that $(v - q'/q)x + p\mathcal{J}$ is well defined because $(v - q'/q)q\mathcal{J} \subset p\mathcal{J}$. Also observe that for all $x \in \mathcal{J}_q$, we have $(q'/q)x + F_{\mathcal{J}}(x) \in \mathcal{J}_{q'}$ up to zero message, i.e., up to a multiple of p. ($\because$ If $x \in q\mathcal{J}$ then $vx = vq\mathcal{J} \subseteq q'\mathcal{J}$, but note that v is defined up to a multiple of p.) It is trivial to see that $qF_{\mathcal{J}}(x) \in p\mathcal{J}$.

Modulus Reduction Procedure

$c(S) = c_0 + c_1 S$ is an input ciphertext with $c_0,\ c_1 \in R_q^\vee$. Let $f_0 \leftarrow F_{R^\vee}(c_0)$, $f_1 \leftarrow t^{-1}F_R(tc_1)$, where we used the bases $\vec{d}$ for $R^\vee$, and $\vec{p}$ for R. Output is $c'(S) = c_0' + c_1 S$, where

$$c_0' = \frac{q'}{q}c_0 + f_0 \mod q'R^\vee, \tag{11.2}$$

$$c_1' = \frac{q'}{q}c_1 + f_1 \tag{11.3}$$

$$= t^{-1}\left(\frac{q'}{q}tc_1 + F_R(tc_1)\right) \mod q'R^\vee. \tag{11.4}$$

Then

$$c_0' + c_1's = \frac{q'}{q}(c_0 + c_1 s) + (f_0 + f_1 s) \tag{11.5}$$

$$= \frac{q'}{q}e + (f_0 + (tf_1)s') \mod q'R^\vee. \tag{11.6}$$

We define $e' = q'/q \cdot e + (f_0 + f_1 s)$. Note that $e' = \frac{q'}{q}e \mod pR^\vee$, since $qf_0 + q(tf_1)s' \in pR^\vee$. The added error term $f = (f_0 + f_1 s)$ is 0-subgaussian with parameter

$$p\sqrt{2\pi}(\mathrm{rad}(m)/m + \hat{m}\|t^{-1}s\|_\infty^2)^{1/2}, \tag{11.7}$$

and

$$\|f\|_2 \le p\sqrt{n}(\sqrt{\mathrm{rad}(m)/m} + \sqrt{\hat{m}}\|t^{-1}s\|_\infty)$$

always if we use coordinate-wise randomized rounding to a coset of $pR^\vee$ (respectively, pR) using the basis $p\vec{d}$ (respectively, $p\vec{p}$) because of the definition of coordinatewise randomized rounding defined at discretization, and the fact that if $\mathbf{f} = \sum f_i \mathbf{b}_i$ is the output, then $|f_i| \leq 1$.

Key Switching

$c(S)$: degree-k ciphertext,
$I = (R^\vee)^k$, $d = k+1$,
$\vec{s} = (s^0, \ldots, s^k) \in R^{[d]}$,
$\vec{c} \in I_q^{[d]}$: coefficient vector of a valid degree-k ciphertext $c(S)$, where decryption $c(s) = \langle \vec{c}, \vec{s} \rangle = e \mod qI$ for some short $e \in t^{-k}\mu + pI$.

Think of $e \in I = (R^\vee)^k$ as an element in the super lattice $\hat{m}^{1-k} R^\vee \supset I$. Then

$$\hat{m}^{k-1} e = \left\langle t \hat{m}^{k-1} \vec{c}, t^{-1} \vec{s} \right\rangle . \tag{11.8}$$

Let $\vec{y} = t\hat{m}^{k-1}\vec{c} \in R_q^{[d]}$, $l = \lceil \log_2 q \rceil$, and define

$$\begin{aligned} \mathbf{g} &= (1, 2, 4, \ldots, 2^{l-1}) \in \mathbb{Z}_q^{[l]}, & (11.9) \\ G &= I_{[d]} \otimes g^T \in \mathbb{Z}_q^{[d]\times[dl]}. & (11.10) \end{aligned}$$

Find short $\vec{x} \in R^{[dl]}$ such that $G\vec{x} = \vec{y} \in R_q^{[d]}$. (To find such short $\vec{x}$, we do need a good basis for $\Lambda^\perp(G)$, which we have; see lemma 23.) We have

$$\hat{m}^{k-1} e = \left\langle \vec{y}, t^{-1} \vec{s} \right\rangle = \left\langle \vec{x}, t^{-1} G^T \vec{s} \right\rangle \mod qR^\vee . \tag{11.11}$$

Hint is a collection of independent degree -1 ciphertext $h_i(S')$ for each $i \in [dl]$ given below. (Note that the original secret was $(s^0, s^1, \ldots, s^k)$. What we are going to do can be thought of as the encryption of each s^j in an l-vector.)

$$h_i(s') \leftarrow Enc_{s'}(0) + t^{-1}(G^T\vec{s})_i \mod qR^\vee, \tag{11.12}$$

i.e., we generate degree -1 encryptions of 0 and simply add entries of $t^{-1}G^T\vec{s}$ to their constant terms.

$$h_i(S') = f_i + t^{-1}(G^T\vec{s})_i \tag{11.13}$$

for some short $f_i \in pR^\vee$. For $\vec{f} = (f_i)_{i\in[dl]}$, we define

$$F := \max_{i \in \mathbb{Z}_m^*} \left(\sum_{j=1}^{dl} |\sigma_i(f_j)|^2 \right)^2 . \tag{11.14}$$

<u>Claim:</u> If all the entries $f_j \in R^\vee$ are δ-subgaussian with parameter s for some $\delta = \mathcal{O}(1)$, then

$$F \leq Cs \cdot \max(\sqrt{dl}, \omega(\sqrt{\log n})) \tag{11.15}$$

except with $negl(n)$ probability.

Proof.

$$\begin{aligned}
& \max_{i\in\mathbb{Z}_m^*}\left(\sum_{j=1}^{dl}|\sigma_i(f_j)|^2\right) && (11.16)\\
= \;& \max_{i\in\mathbb{Z}_m^*}\left(\sum_{j=1}^{dl}\mathrm{Re}(\sigma_i(f_j))^2+\sum_{j=1}^{dl}\mathrm{Im}(\sigma_i(f_j))^2\right) && (11.17)\\
\leq \;& 2\max_{i\in\mathbb{Z}_m^*}\max\left\{\sum_{j=1}^{dl}\mathrm{Re}(\sigma_i(f_j))^2,\sum_{j=1}^{dl}\mathrm{Im}(\sigma_i(f_j))^2\right\}. && (11.18)
\end{aligned}$$

Then previous estimation on $Pr(\sum_i x_i^2 > r)$ implies the claim, since $\mathrm{Re}(\sigma_i(f_j))$ and $\mathrm{Im}(\sigma_i(f_j))$ are δ-subgaussian with parameter $s/\sqrt{2}$. □

Remark 11.3.3. $\frac{1}{\sqrt{2}}(x_i + x_{m-i}) = \sqrt{2}\mathrm{Re}(x_i)$ and similarly for $\sqrt{2}\mathrm{Im}(x_i)$, and $B = \frac{1}{\sqrt{2}}\begin{pmatrix} I & \sqrt{-1}J \\ J & -\sqrt{-1}I \end{pmatrix}$ is unitary basis of H, so $\sqrt{2}\mathrm{Re}(\sigma(\cdot))$ and $\sqrt{2}\mathrm{Im}(\sigma(\cdot))$ are Gaussian with parameter s.

Key Switching Procedure

Input $\vec{c}\in I_q^{[d]}$, compute $\vec{y} = t\hat{m}^{k-1}\vec{c}\in R_q^{[d]}$, generate a short $\vec{x}\in R^{[dl]}$ such that $G\vec{x}=\vec{y}$. Output the degree -1 cyphertext

$$c'(S') = \sum_{i\in[dl]} x_i h_i(S'). \tag{11.19}$$

Then

$$\begin{aligned}
c'(s') &= \sum x_i(f_i + t^{-1}(G^T\vec{s})_i) && (11.20)\\
&= \left\langle \vec{x},\vec{f}\right\rangle + \langle \vec{x}, t^{-1}G^T\vec{s}\rangle && (11.21)\\
&= \left\langle \vec{x},\vec{f}\right\rangle + \hat{m}^{k-1}e \mod qR^\vee. && (11.22)
\end{aligned}$$

Hence, the noise term is $e' = \left\langle \vec{x},\vec{f}\right\rangle + \hat{m}^{k-1}e$. Note that $e' = \hat{m}^{k-1}e$ modulo $pR^\vee$, since $f_i\in pR^\vee$. e' is a relatively short element of $R^\vee$, since e was short in $\hat{m}^{1-k}R^\vee$, and $\vec{x}$ and $\vec{f}$ are also short in $R^\vee$ by construction. To choose a short $\vec{x}$ such that $G\vec{x}=\vec{y}$ for a given $\vec{y}\in R_q^{[d]}$, it suffices to find a short basis of $\Lambda^\perp(G)$.

Lemma 11.3.4. There is an efficiently computable $\mathbb{Z}$-basis $Z\in R^{[dl]\times[dln]}$ of $\Lambda^\perp(G)$ satisfying the following bounds, where $\|\widetilde{Z}\|_2$ denotes the largest l_2-norm of the Gram-Schmidt orthogonalized vector $\widetilde{Z}$. If q is a power of 2, then $s_1(Z)\leq 3\sqrt{\hat{m}}$ and $\|\widetilde{Z}\|_2 = 2\sqrt{n}$, otherwise $s_1(Z)\leq\sqrt{(9+wt_2(q))\hat{m}}$ and $\|\widetilde{Z}\|_2=\sqrt{5n}$, where $wt_2(q)$ denotes the number of 1s in binary expansion of q.

Proof. Consider the integral lattice

$$\mathcal{L}^\perp(G) = \{\vec{z}\in\mathbb{Z}^{[dl]} : G\vec{z} = 0\in\mathbb{Z}_q^{[d]}\}. \tag{11.23}$$

Define $S_g \in \mathbb{Z}^{[l]\times[l]}$ as

$$S_g = \begin{pmatrix} 2 & & & & \\ -1 & 2 & & & \\ & -1 & \ddots & & \\ & & & 2 & \\ & & & -1 & 2 \end{pmatrix} \tag{11.24}$$

if $q = 2^l$, and otherwise

$$S_g = \begin{pmatrix} 2 & & & & q_0 \\ -1 & 2 & & & q_1 \\ & \ddots & \ddots & & \vdots \\ & & \ddots & 2 & q_{l-2} \\ & & & -1 & q_{l-1} \end{pmatrix}, \tag{11.25}$$

where $q = \sum_{i\in[l]} q_i 2^i$ is the binary representation of q, with $q_i \in \{0,1\}$. The columns of S_q form a basis of $\mathcal{L}^{\perp}(g^T)$, since the columns of S_q are linearly independent and $\det S_g = 2^l = \det(\mathcal{L}^{\perp}(g^T))$ if $q = 2^l$, and also $\det S_g = q$ in general if we consider the expansion of $\det S_g$ with respect to the last column.

The Gram-Schmidt Orthogonalization from earlier with $q = 2^l$ is

$$\widetilde{S} = \begin{pmatrix} 2 & & & \\ & 2 & & \\ & & \ddots & \\ & & & 2 \end{pmatrix} \text{ if } q = 2^l. \tag{11.26}$$

If q not a power of 2, we use the standard Gram-Schmidt Orthogonalization. Then

$$\|\widetilde{S}_i\|^2 = 1 + \frac{4^i}{\sum_{j<i} 4^j} = \frac{4-4^{-i}}{1-4^{-i}}(<5) \quad \text{for } i = 1,\dots,l-1, \tag{11.27}$$

$$\|\widetilde{S}_l\|^2 = \frac{3q^2}{4^l-1} < 3. \tag{11.28}$$

(To compute $\|\widetilde{S}_l\|^2$, note that $S_i \perp \alpha$ for $i = 1,2,\dots,l-1$, where $\alpha = (1,2,\cdots,2^{l-1})$, hence

$$\|\widetilde{S}_l\|^2 = \frac{\langle s_l,\alpha\rangle^2}{\|\alpha\|^2} = \frac{q^2}{\sum_{j=0}^{l-1} 4^j} = \frac{3q^2}{4^l-1}.) \tag{11.29}$$

By definition,

$$s_1(A) = \max_{u\neq 0} \frac{\|Au\|}{u}. \tag{11.30}$$

When $q = 2^l$,

$$S_g = \begin{pmatrix} 2 & & & \\ & 2 & & \\ & & \ddots & \\ & & & 2 \end{pmatrix} (= A_1) + \begin{pmatrix} 0 & & & \\ -1 & 0 & & \\ & \ddots & \ddots & \\ & & -1 & 0 \end{pmatrix} (= A_2).$$

$S_g(u) = A_1 u + A_2 u$, where $\|u\| = 1$. Hence,

$$\|S_g u\| \le \|A_1 u\| + \|A_2 u\| \le 2 + 1 = 3.$$

When $q \neq 2^l$, we consider S_g^T.

$$\begin{pmatrix} 2 & -1 & & & \\ & 2 & -1 & & \\ & & \ddots & & \\ & & & 2 & -1 \\ q_0 & q_1 & \cdots & q_{l-2} & q_{l-1} \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{l-2} \\ u_{l-1} \end{pmatrix} \tag{11.31}$$

$$= \begin{pmatrix} 2u_0 - u_1 \\ 2u_1 - u_2 \\ \vdots \\ 2u_{l-2} - u_{l-1} \\ q_0 u_0 + \cdots + q_{l-1} u_{l-1} \end{pmatrix} \tag{11.32}$$

$$= 2 \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{l-2} \\ 0 \end{pmatrix} - \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_{l-1} \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ q_0 u_0 + \cdots + q_{l-1} u_{l-1} \end{pmatrix}, \tag{11.33}$$

where $h = (q_0, q_1, \cdots, q_{l-1})$, hence $\|h\| = wt_2(q)$. Then

$$\|S_g^T u\|^2 \le (3\|u\|)^2 + \|h\|^2 \|u\|^2,$$

so

$$\|S_g^T u\| < \sqrt{9 + wt_2(q)} \|u\|.$$

Now we claim that

$$Z = S \otimes \vec{p}^T = I_{[d]} \otimes S_g \otimes \vec{p}^T \in R^{[dl] \times [dln]}$$

is a $\mathbb{Z}$-basis of $\Lambda^\perp(G)$ satisfying the bounds in the lemma, where $\vec{p}$ is the powerful basis of R. Because

$$\begin{aligned} s_1(Z) &= s_1(S) \cdot s_1(\vec{p}) = s_1(S)\sqrt{\hat{m}}, & (11.34) \\ \|\widetilde{Z}\|_2 &= \|\widetilde{S}\|_2 \|\widetilde{CRT_m}\|_2 = \|\widetilde{S}\|_2 \sqrt{n}, & (11.35) \end{aligned}$$

we have proved the lemma. □

Remark 11.3.5. Let $A \in \mathbb{Z}_q^{[h] \times [k]}$ be given. Then for any $\mathbb{Z}$-basis B of $\mathcal{L}^\perp(A) \subset \mathbb{Z}^{[k]}$ and a $\mathbb{Z}$-basis $\vec{b}$ of R, $B \otimes \vec{b}^T$ is a $\mathbb{Z}$-basis of $\Lambda^\perp(A) \subset R^{[k]}$. To prove this, let $\vec{z} \in \Lambda^\perp(A)$, i.e., $A\vec{z} = 0 \in R_q^{[h]}$. Since $\vec{z} \in R^k$ and $\vec{z} = (\zeta_1, \ldots, \zeta_k)$, where $\zeta_i \in R$,

$$\zeta_i = \sum a_{ij} b_j, \quad i = 1, \ldots, k, a_{ij} \in \mathbb{Z}. \tag{11.36}$$

Then

$$\vec{z} = \sum b_j \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{kj} \end{pmatrix} = \sum b_j \cdot \mathbf{a}_j,$$

where $\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{kj} \end{pmatrix} = \mathbf{a}_j$. Hence, $A\vec{z} = 0$ implies $A\mathbf{a}_j = 0 \in \mathbb{Z}_q^{[h]}$, i.e., $\mathbf{a}_j \in \mathcal{L}^{\perp}(A)$, so $\mathbf{a}_j$ can be written uniquely as a $\mathbb{Z}$-linear combination of basis elements in B, i.e., $B \otimes \vec{b}^T$ forms a basis of $\Lambda^{\perp}(A) \subseteq R^{[k]}$.

Part III

Multilinear map

Chapter 12

Multilinear maps

12.1 Why multilinear map?

Two-party non-interactive key exchange (2-party NIKE, Diffie-Hellman key exchange) protocol

- Publish a cyclic group G (i.e., generator g of order q) where discrete log problem is hard.
- Alice chooses a random $x_1 \in \mathbb{Z}_q$, publishes $y_1 = g^{x_1}$
- Bob chooses a random $x_2 \in \mathbb{Z}_q$, publishes $y_2 = g^{x_2}$.
- Alice and Bob compute agreed secret key $K = g^{x_1 x_2} = {y_1}^{x_2} = y_2^{x_1}$.
- Security: Computational Diffie-Hellman problem (CDH), i.e., given g, g^{x_1}, g^{x_2}, compute $g^{x_1 x_2}$.

Wish to have an N-multiparty version: G, G_T are groups where Discrete log is hard, and there is an efficient $(N-1)$-linear map $e : G^{N-1} \to G_T$ such that

$$e(g^{x_1}, \ldots, g^{x_{N-1}}) = e(g, \ldots, g)^{x_1 \cdots x_{N-1}}$$

for all $x_1, \ldots, x_{N-1} \in \mathbb{Z}_q$.

Then we obtain N-party NIKE:

- Publish cyclic groups G and G_T (with generators g and g_T, of order q), where DL-problem is hard, and an efficient $(N-1)$ linear map e.
- For $i = 1, \ldots, N$, party P_i chooses $x_i \in \mathbb{Z}_q$ and publishes $y_i = g^{x_i}$.
- All parties can compute the agreed secret key

$$\begin{aligned} K &= e(y_2, y_3, \ldots, y_N)^{x_1} && (12.1) \\ &= e(g, g, \ldots, g)^{x_1 x_2 \cdots x_N}. && (12.2) \end{aligned}$$

- Security: Hardness of Multilinear CDH problem (MCDH), i.e., given $g, g^{x_1}, \ldots, g^{x_N}$, compute $e(g, \ldots, g)^{x_1 \cdots x_N}$.

12.2 Grag-Gentry-Halevi (GGH) Graded Encoding Scheme

High level description

- $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$, where n is a power of 2.
- Publish rings R_g, R_q, and some public parameters of $N-1$ Graded Encoding Scheme.
- For $i = 1, \ldots, N$, party P_i chooses $x_i \in R_g$, publishes $y_i = Enc_1(par, x_i : \rho_i)$, i.e., level 1 encoding of x_i with noise ρ_i with some encoding scheme.
- We require

$$Enc_1(par, x_1 : \rho_1) \cdots Enc_1(par, x_k : \rho_k) = Enc_k(par, x_1 \cdots x_k : \rho) \tag{12.3}$$

  and

$$x \cdot Enc_k(par, z : \rho) = Enc_k(par, x \cdot z : \rho). \tag{12.4}$$

- Noise-clearing Extraction process at level k

$$Ext(par, Enc_k(par, x : \rho)) = r(x) \in \{0,1\}^n \tag{12.5}$$

  should be independent of randomness ρ, and we require output $x(x) \in \{0,1\}^n$ to be uniform for uniform input $x \leftarrow U(R_g)$.

- Then all parties have agreed secret key

$$\begin{aligned} K &= Ext(par, Enc_{N-1}(par, x_1 \cdots x_N : \rho)) && (12.6)\\ &= Ext(par, x_1 y_2 \cdots y_N). && (12.7) \end{aligned}$$

$$\begin{aligned} (\because x_1 y_2 \cdots y_N &= x_1 Enc_1(par, x_1 : \rho_1) \cdots Enc_1(par, x_k : \rho_k) && (12.8)\\ &= x_1 Enc_{N-1}(x_2 \cdots x_N : \rho) && (12.9)\\ &= Enc_{N-1}(x_1 x_2 \cdots x_k : \rho)) && (12.10) \end{aligned}$$

- Security: Extraction of Graded computational Diffie-Hellman problem (Ext-GCDH): Given

$$y_1 = Enc_1(par, x_1 : \rho_1), \cdots, y_N = Enc_1(par, x_N : \rho_N),$$

  compute

$$Ext(par, Enc_{N-1}(par, x_1 \cdots x_N : \rho)).$$

Construction of $Enc_1, \cdots, Enc_k$

Public parameters

- Sample a small $g \hookleftarrow D_{R,\sigma}$ until $\|g^{-1}\| \leq lg^{-1}$ and $I = \langle g\rangle$ is prime, where $D_{R,\sigma}$ is discrete Gaussian with variance σ. Define encoding domain $R_g = R/\langle g\rangle$.
- Sample $z \hookleftarrow U(R_g)$.

- Sample a level 1 encoding of 1, i.e., set $y = [a \cdot z^{-1}]_q$ with $a \hookleftarrow D_{1+I,\sigma'}$.
- Sample m_r level-1 encodings of 0, i.e., set $s_j = [b_j \cdot z^{-1}]_q$ with $b_j \hookleftarrow D_{I,\sigma'}$ for all $j \leq m_r$.
- Sample $h \hookleftarrow D_{R,\sqrt{q}}$ and define a zero-testing parameter $p_{zt} = [\frac{h}{g} z^k]_q \in R_q$.
- Return $par = (n, q, y, \{x_j\}_{j \leq m_r})$ and p_{zt}.

Remark 12.2.1.

$$\begin{aligned} R = \mathbb{Z}[x]/\langle x^n + 1\rangle \quad &\leftrightarrow \quad \mathbb{Z}^n && (12.11) \\ \sum_{i=0}^{n-1} a_i x^i \quad &\leftrightarrow \quad (a_0, \cdots, a_{n-1}) && (12.12) \\ I(\text{ideal}) \subset R \quad &\leftrightarrow \quad \text{sublattice of } \mathbb{Z}^n && (12.13) \end{aligned}$$

- poly(n)-ideal lattice SVP is assumed to be still difficult even against quantum computer. But note that Gap-SVP for ideal lattice is trivial.
- R could be imbedded in $\mathbb{C}^n$ via the canonical map $\sigma = (\sigma_1, \cdots, \sigma_n)$.
- But when n is a power of 2, the coefficient embedding and the canonical embedding are isometric up to the constant $\sqrt{n}$.
  If $\alpha(z) = a_0 + a_1 z + \cdots + a_{n-1}z^{n-1}$, then

$$\begin{aligned} &(\alpha(\zeta), \alpha(\zeta^3), \cdots, \alpha(\zeta^{2n-1})) && (12.14) \\ &= (a_0, a_1, \cdots, a_{n-1}) \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \zeta & \zeta^3 & \cdots & \zeta^{2n-1} \\ \zeta^2 & \zeta^{2\cdot 3} & \cdots & \zeta^{2(2n-1)} \\ \vdots & \vdots & \cdots & \vdots \\ \zeta^{n-1} & \zeta^{(n-1)3} & \cdots & \zeta^{(n-1)(2n-1)} \end{pmatrix}, && (12.15) \end{aligned}$$

  where $\zeta = e^{2\pi i/n}$ and $n = 2^k$. Note that

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \zeta & \zeta^3 & \cdots & \zeta^{2n-1} \\ \zeta^2 & \zeta^{2\cdot 3} & \cdots & \zeta^{2(2n-1)} \\ \vdots & \vdots & \cdots & \vdots \\ \zeta^{n-1} & \zeta^{(n-1)3} & \cdots & \zeta^{(n-1)(2n-1)} \end{pmatrix} \qquad (12.16)$$

  is unitary up to $\sqrt{n}$. Hence,

$$\begin{aligned} \|\sigma(\alpha(z))\| \quad &= \quad \sqrt{n}\sqrt{|a_0|^2 + \cdots + |a_{n-1}|^2} && (12.17) \\ &= \quad \sqrt{n}\|\alpha\|. && (12.18) \end{aligned}$$

Level-1 encoding $Enc_1(par, e)$

- Given level-0 $e \in R$: $e \hookleftarrow D_{R,\sigma'}$, $u' = [ey]_q$, hence $u' = [c'/z]_q$ with $c' \in e + I$ (Note that $e = [e]_{\langle g \rangle} + ge_H$ for some $e_H \in R$, where $[e]_g$ is the unique coset representative in P_g, and $P_g = \{\sum_{i=0}^{n-1} c_i x^i g : c_i \in [-\frac{1}{2}, \frac{1}{2})\}$. Also note that $(g, xg, \cdots, x^{n-1}g)$ is a short $\mathbb{Z}$-basis of the ideal lattice $\langle g \rangle$.)

- Rerandomize: Sample small $\rho_j \hookleftarrow D_{\mathbb{Z},\sigma_1^*}$ for $j \leq m_r$, and return $u = [u' + \sum_{j=1}^{m_r} \rho_j x_j]_q$. Hence, $u = [c/z]_q$ with $c \in e + I$ and $c = c' + \sum \rho_j b_j$.

Multiplying encodings

Given a level-k_1 encoding $u_1 = [c_1/z_1^k]_q$ of e_1 and a level-k_2 encoding $u_2 = [c_2/z^{k_2}]_q$ of e_2, $u = [u_1 \cdot u_2]_q$ is a level-$(k_1 + k_2)$ encoding of $[c_1 \cdot c_2]_g$. Note that $u_1 \cdot u_2 = [c_1 c_2 / z^{k_1+k_2}]_q$ and $c_1 \cdot c_2 \in e_1 \cdot e_2 + I$.

Extraction at level k $Ext(par, u)$

Given a level-k encoding $u = [c/z^k]_q$, return

$$\begin{aligned} v &= \text{ up to } l\text{th most significant bit of } [p_{zt} u]_q \text{ with } l < (\frac{1}{4} - \varepsilon) \log q \\ &=: MSB_l([p_{zt} \cdot u]_q). \end{aligned}$$

Correctness of extraction

- At level 1: if $c = [c]_g + gr$ for some small $r \in R$, then

$$v = MSB_l\left(\frac{h}{g}([c]_g + gr)\right) = MSB_l\left(\frac{h}{g}[c]_g + hr\right),$$

  which is equal to $MSB_l(\frac{h}{g}[c]_g)$ with high probability if $q > \|r\|^8$. Since $h \sim \sqrt{q}$, $\|hr\| \sim \sqrt{q}\|r\|$. If $q > \|r\|^8$, then $\sqrt{q}\|r\| < q^{\frac{1}{2}+\frac{1}{8}} = q^{\frac{5}{8}}$. Hence, the noise term hr does not contribute to the most significant lth bit if $l < (\frac{1}{4} - \varepsilon) \log q$, since $q^{\frac{5}{8}}$ contributes up to $\frac{5}{8} \log q$ least significant bits.

- After k multiplications: for $u_i = [\frac{x_i + gr_i}{z}]_q$, where $i = 1, \cdots, k$, we have

$$u = u_1 u_2 \cdots u_k = \left[\frac{x + gr}{z^k}\right]_q,$$

  where $x = x_1 \cdots x_k$. Then we require r to satisfy

$$\begin{aligned} \|r\| &= \mathcal{O}(2^k \|(gr_1) \cdots (gr_k)\|) && (12.19) \\ &\quad (\because 2^k \text{ because there are } 2^k \text{ terms}) \\ &= \mathcal{O}((\mathrm{poly}(n) N)^k) < q^{1/8}, && (12.20) \end{aligned}$$

  where $N := \max_i \|gr_i\|$, i.e., $\mathcal{O}(\max_i \|gr_i\|) < q^{1/8k} / \mathrm{poly}(n)$.

Security of GDH for GGH scheme

Known attacks need a small multiple of g, dg ($\|dg\| < q$).

Note: From public parameters, it is easy to compute a basis for the ideal $\langle g \rangle$, even though g is a secret. But usually the bases thus found are rather long, so it is difficult to find a short element dg in $\langle g \rangle$.

Attack on Graded Discrete Log problem. Given $u = Enc_1(par, x) = \left[\frac{x+rg}{z}\right]_q$ for small r.

- Compute $p'_{zt} := [dgp_{zt}]_q = [dg\frac{h}{g}z^k]_q = [dhz^k]_q$.
- Let $u' = [uy^{k-1}]_q = [\frac{x+r'g}{z^k}]_q$, $y' = [y^k]_q = [\frac{1+r'_y g}{z^k}]_q$.
- Compute $u'' := [u'p'_{zt}]_q = dh(x + r' \cdot g) \in R$, $y'' := [y'p'_{zt}]_q = dh(1 + r'_y \cdot g) \in R$.
- Using a basis for $\langle g \rangle$ obtained from public parameters, it is easy to compute a (in general very large) representation $x' \in R$, where $x' = u''y''^{-1} \mod \langle g \rangle$, so $x' = x \mod \langle g \rangle$ since $u''y''^{-1} = x \mod \langle g \rangle$.
- Compute a small representation $x'' = x' \mod \langle dg \rangle$. Then $x'' = x \mod \langle g \rangle$.

Note: $\langle dg \rangle$ is a sublattice of $\langle g \rangle$, and we have a short basis for the ideal lattice $\langle dg \rangle$, but in general not for the ideal lattice $\langle g \rangle$.

Chapter 13

GGHLite scheme for k-graded encoding

Public Parameter Generation

- Sample $g \hookleftarrow D_{R,\sigma}$ until $\|g^{-1}\| \leq l_{g^{-1}}$ and $I = \langle g \rangle$ is prime.
- Sample $z \in U(R_q)$.
- Sample a level-1 encoding of 1: $y = [az^{-1}]_q$ with $a \hookleftarrow D_{1+I,\sigma'}$.
- Sample $B = (b_1, b_2) \in R \times R$ from $(D_{I,\sigma'})^2$. If $\langle b_1, b_2 \rangle \neq I$ or $\sigma_n(\operatorname{rot} B) < l_b$, then resample.
  Note:

$$\operatorname{rot} B : R \times R \rightarrow R \tag{13.1}$$
$$(x, y) \rightarrow xb_1 + yb_2 \tag{13.2}$$

  and $\sigma_n(\operatorname{rot} B)$ is the smallest singular value of $\operatorname{rot} B$ as a linear map.

- Define level-1 encodings of 0:

$$x_1 = [b_1 \cdot z^{-1}]_q, \qquad x_2 = [b_2 \cdot z^{-1}]_q. \tag{13.3}$$

- Sample $h \hookleftarrow D_{R,\sqrt{q}}$, and define a zero test parameter $p_{zt} = [\frac{h}{g} z^k]_q \in R_q$.
- Return parameters $= (n, q, y, x_1, x_2, p_{zt})$.

Level-1 encoding $Enc(par, e)$

Given a level-0 $e \in R$,

- Encode e at level-1: compute $u' = [ey]_q$.
- Return $u = [(u' + \rho_1 x_1 + \rho_2 x_2)/z]_q$ with $\rho_1, \rho_2 \hookleftarrow D_{R,\sigma_1^*}$.
- Hence, $u' + \rho_1 x_1 + \rho_2 x_2$ is in $D_{I+\rho}$, $\sigma_1^* B^T$, ey.

Formalizing Re-randomization Security

Informal requirement: Prevent correlation of statistical properties of re-randomized encoding with encoded element.

Formal requirement: Breaking Ext-GCDH problem is as hard as breaking canonical Ext-GCDH problem.

- Ext-GCDH: Given public parameters and $y_1 = [e_1 y + \rho_{11} x_1 + \rho_{21} x_2]_q, \cdots, y_N = [e_N y + \rho_{1N} x_1 + \rho_{2N} x_2]_q$, compute

$$Ext(par, Enc_{N-1}(par, e_1 \cdots e_N : \rho)) = MSB_l(p_{zt} \cdot y_1 \cdots y_N). \tag{13.4}$$

- Canonical Ext-GCDH: Given public parameters and $y_1 = [c_1 z^{-1}]_q, \cdots, y_N = [c_N z^{-1}]_q$ with $c_i \hookleftarrow D_{I+e_i, \sigma^* B^T}$ for $i = 1, \cdots, N$, compute

$$Ext(par, Enc_{N-1}(par, e_1 \cdots e_N : \rho)) = MSB_l(p_{zt} \cdot y_1 \cdots y_N). \tag{13.5}$$

Remark 13.0.2. The difference between Ext-GCDH and canonical Ext-GCDH is that sampling in Ext-GCDH is from a shifted Gaussian (shifted by $e_i \cdot y$), while sampling in canonical Ext-GCDH is from a fixed origin centered Gaussian, but with a shifted lattice (by e_i).

Theorem 13.0.3. This requirement is satisfied under suitable parameter conditions.

D_1: The distribution of $y_i = [v_i/z]_q$ in Ext-GCDH problem

- v_i distribution is a shifted Gaussian $D_{I+e_i, \sigma_1^* B^T, c_i'}$ with small shifted center $c_i' = e_i y$.

D_2: The distribution of $y_i = [v_i/z]_q$ in canonical Ext-GCDH problem

- v_i distribution is $D_{I+e_i, \sigma_1^* B^T}$ – which has no shift of center.

The original strong GCDH requirement was based on the statistical distance (SD) Δ: They required

$$\Delta(D_1, D_2) := \sum_x |D_1(x) - D_2(x)| < 2^{-\lambda}. \tag{13.6}$$

Problem with the strong requirement

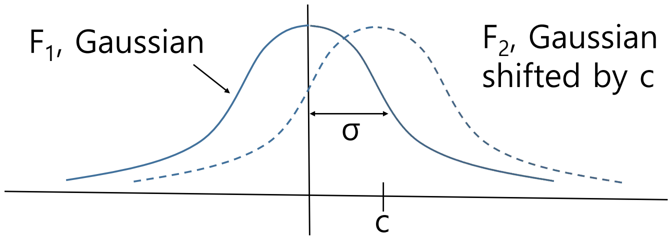
We ask any adversary A with success probability ε against Ext-GCDH problem. Then the success probability ε' is still small (exponentially) against the canonical Ext-GCDH. Since

$$|\varepsilon - \varepsilon'| < \Delta(D_1, D_2), \tag{13.7}$$

we have

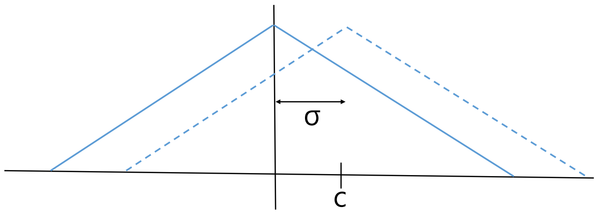
$$\varepsilon - \Delta(D_1, D_2) < \varepsilon' < \varepsilon + \Delta(D_1, D_2). \tag{13.8}$$

Hence, we need the statistical distance $\Delta(D_1, D_2) < 2^{-\lambda}$ exponentially small. Consequently, we need $\frac{\sigma_1^*}{\|c_1'\|} = 2^{\Omega(\lambda)}$ (called exponential drowning). Note that



$$\Delta(F_1, F_2) = O\left(\frac{c}{\sigma}\right). \tag{13.9}$$

Hint:



(Approximated version of the above)

Security analysis of GGHLite is based on Renyi divergence (RD) R

$$R(D_1 \| D_2) := \sum_x D_1^2(x)/D_2(x) \tag{13.10}$$

Remark on Renyi divergence: On $\mathbb{R}^n$,

$$R(P\|Q) = \int_{\mathbb{R}^n} \frac{P^2(x)}{Q(x)} dx = \mathbb{E}_P\left(\frac{P}{Q}\right).$$

Note that

$$\frac{\left(\int_A P(x)dx\right)^2}{\int_A Q(x)dx} < \int_A \frac{P^2(x)}{Q(x)} dx < R(P\|Q). \tag{13.11}$$

(For a general subset A, the first inequality follows from the Cauchy-Schwarz inequality since $P(x) = \frac{P(x)}{\sqrt{Q(x)}}\sqrt{Q(x)}$.) Hence, $Q(A) \geq P(A)^2/R(P\|Q)$.

Security analysis of GGHLite based on Renyi divergence

Any adversary A with success probability ε against Ext-GCDH problem has success probability ε' against canonical Ext-GCDH problem with

$$\varepsilon' \geq \varepsilon^2/R(D_1\|D_2)^2. \tag{13.12}$$

Hence, we require only that $R(D_1\|D_2)$ is poly(λ). Then $\epsilon' \sim 2^{-\lambda}$ implies $\varepsilon \sim 2^{-\lambda}$.

Lemma 13.0.4. For any n-dimensional lattice $\Lambda \subset \mathbb{R}^n$ and rank n matrix $S \in \mathbb{R}^{m\times n}$, let P be the center-shifted Gaussian distribution $D_{\Lambda,S,w}$, and Q the center-shifted Gaussian distribution $D_{\Lambda,S,z}$ for some $w, z \in R^n$. If $w, z \in \Lambda$, let $\varepsilon = 0$. Otherwise fix $\varepsilon \in (0, 1)$ and assume that $\sigma_n(S) \geq \eta_\varepsilon(\Lambda)$. Then

$$\begin{aligned} R(P\|Q) \;&\in\; \left[\left(\frac{1-\varepsilon}{1+\varepsilon}\right)^2, \left(\frac{1+\varepsilon}{1-\varepsilon}\right)^2\right] \exp(2\pi\|S^{-T}(w-z)\|^2) && (13.13)\\ &\subset\; \left[\left(\frac{1-\varepsilon}{1+\varepsilon}\right)^2, \left(\frac{1+\varepsilon}{1-\varepsilon}\right)^2\right] \exp\left(\frac{2\pi\|(w-z)\|^2}{\sigma_n(S)^2}\right) && (13.14)\end{aligned}$$

(refer the paper [LSS14] on GGHLite for the proof.)

Hence, the lemma implies that

$$R(D_1\|D_2) \leq \exp\left(\frac{2\pi\|c_1'\|^2}{\sigma_n(\sigma_1^* B^T)^2}\right). \tag{13.15}$$

For the requirement $R(D_1\|D_2) \leq$ poly(λ), we can use $\frac{\sigma_1^*}{c_1'} = \mathcal{O}(1/|\log\lambda|)$.

In our scheme, $v_i = [e_i a + \rho_1 b_1 + \rho_2 b_2/z]_q$ with $\rho_i \hookleftarrow D_{R,\sigma_1^*}$. Hence, we have to show that

$$\rho_1 b_1 + \rho_2 b_2 \approx D_{I,\sigma_1^* B^T}, \tag{13.16}$$

where $B = [b_1, b_2] = g[t_1, t_2] \in R^2$.

- Step 1. We show $[t_1, t_2]R^2 = R$ with nonzero probability.

  Remark 13.0.5. It is the probability that two random algebraic integers are coprime $\approx \zeta_R(2)^{-1}$ as in the integer case. (Let n_1, n_2 be random integers, and p a prime. Then the probability that both n_1 and n_2 has p as a common factor is $\frac{1}{p^2}$. Hence, the probability that the pair n_1, n_2 is coprime is given by $\prod_{p\,\mathrm{prime}}\left(1-\frac{1}{p^2}\right)$, which is $\zeta(2)^{-1}$.)

  Remark 13.0.6. $[t_1, t_2]R^2 \neq R$ is non-negligible for $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$, where n is even, since each random element of R falls in the ideal $\langle x + 1\rangle$ with probability $\frac{1}{2}$, hence both t_1, t_2 get stuck in $\langle x + 1\rangle$ with probability $\frac{1}{4}$. ($h = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in R$ is defined up to a multiple of $(x^n + 1)$, i.e., if $\tilde{h} = h + f(x)(x^n + 1)$ in R for some polynomial $f(x)$, then $\tilde{h} = h$ in R. Hence, $h \in \langle x + 1\rangle$ if and only if $h(-1) = 0$ for some $f(x)$, i.e., there exists $f(x)$ such that

  $$a_0 - a_1 + \cdots \pm a_{n-1} + f(-1)2 = 0, \tag{13.17}$$

  that is, if $a_0 - a_1 + \cdots \pm a_{n-1}$ is even.)

- Step 2. Let $A_T = \{V \in R^2 : TV = [t_1, t_2]V = 0\}$. If $\sigma_1^* > \eta_\varepsilon(A_T)$, then $\rho_1 t_1 + \rho_2 t_2$ is within SD 2ε of $D_{R,\sigma_1^* T^t}$, which comes from discrete Gaussian leftover hash lemma.

Chapter 14

Cryptanalysis of GGH map

We follow the notations in Steinfeld's lecture slides. We only explain essential parts of the cryptanalysis due to Yupu Hu and Huiwen Jia [Hu15].

14.1 Schematic description of the cryptanalysis

1. From public noised encoding V of secret v, one generates an equivalent secret, $v^{(0)}$, of which the noise $v^{(0)} - v$ is not short in general and $v^{(0)} - v \in \langle g \rangle$.
2. For the product $\prod_{k=1}^{K+1} v^{(k)}$, $\prod_{k=1}^{K+1} v^{(0,k)} - \prod_{k=1}^{K+1} v^{(k)} \in \langle g \rangle$, but not short.
3. Key step of modified encoding/decoding.
   From $\eta := \prod_{k=1}^{K+1} v^{(0,k)} = \prod_{k=1}^{K+1} v^{(k)} + \xi g$, we obtain

$$\eta''' = (h(1+ag)^K g^{-1}) \prod_{k=1}^{K+1} v^{(k)} + \xi''(1+ag) \quad \bmod q,$$

   where $\xi''(1+ag)$ short. Hence, the higher order bits of η''' are what we want to obtain.

14.2 Generating an equivalent secret

$$\begin{aligned} Y &:= y^{K-1} x^{(1)} p_{zt} \pmod q && (14.1)\\ &= h(1+ag)^{K-1} b^{(1)} && (14.2)\\ X^{(i)} &:= y^{K-2} x^{(i)} x^{(1)} p_{zt} \pmod q && (14.3)\\ &= h(1+ag)^{K-2} (b^{(i)} g) b^{(1)} && (14.4) \end{aligned}$$

Note that RHSs are rather short.

$$\begin{aligned} V &\rightarrow W := V y^{K-2} x^{(1)} p_{zt} \pmod q && (14.5)\\ &\qquad = vY + (u^{(1)} X^{(1)} + u^{(2)} X^{(2)}) : \mathit{short} && (14.6)\\ &\rightarrow W \pmod Y = (u^{(1)} X^{(1)} \pmod Y) + \\ &\qquad\qquad u^{(2)} X^{(2)} \pmod Y)) \pmod Y && (14.7) \end{aligned}$$

From $W \pmod{Y}$, $X^{(1)} \pmod{Y}$, and $X^{(2)} \pmod{Y}$, obtain $W' \in \left\langle X^{(1)}, X^{(2)} \right\rangle$ such that

$$W - W' \pmod{Y} = 0.$$

Denote $W' = u'^{(1)} X^{(1)} + u'^{(2)} X^{(2)}$.

$$\begin{aligned}
v^{(0)} &:= (W - W')/Y && (14.8)\\
&= v + ((u^{(1)} X^{(1)} + u^{(2)} X^{(2)}) - W')/Y && (14.9)\\
&= v + ((u^{(1)} - u'^{(1)}) X^{(1)} + (u^{(2)} - u'^{(2)}) X^{(2)})/Y && (14.10)\\
&= v + ((u^{(1)} - u'^{(1)}) b^{(1)} + (u^{(2)} - u'^{(2)}) b^{(2)} g)\big/(1 + ag). && (14.11)
\end{aligned}$$

Since g and $1 + ag$ are coprime,

$$v^{(0)} - v \in \langle g \rangle .$$

$v^{(0)}$ is called the equivalent secret of v.

14.3 Modified Encoding/Decoding

$$\begin{aligned}
\eta &:= \prod_{k=1}^{K+1} v^{(0,k)} = \prod_{k=1}^{K+1} v^{(k)} + \xi g && (14.12)\\
\eta' &:= Y\eta = Y \prod_{k=1}^{K+1} v^{(k)} + \xi' b^{(1)} g && (14.13)\\
\eta'' &:= \eta' (\mathrm{mod}\ X^{(1)}) && (14.14)\\
\eta'' &= Y \prod_{k=1}^{K+1} v^{(k)} + \xi'' b^{(1)} g && (14.15)
\end{aligned}$$

($\because$ η'' is the sum of η' and a multiple of $X^{(1)}$, and $X^{(1)}$ is a multiple of $b^{(1)} g$.) Note that η'' has size $\sqrt{n} X^{(1)}$ by the definition (mod $X^{(1)}$), and that $Y \prod_{k=1}^{K+1} v^{(k)}$ also small. Hence, $\xi'' b^{(1)} g = \eta'' - Y \prod_{k=1}^{K+1} v^{(k)}$ is small.

$$\begin{aligned}
\eta''' &:= y (x^{(1)})^{-1} \eta'' (\mathrm{mod}\ q) && (14.16)\\
&= (h(1+ag)^K g^{-1}) \prod_{k=1}^{K+1} v^{(k)} + \xi'' (1 + ag) \pmod{q} && (14.17)
\end{aligned}$$

Note that $\xi''(1 + ag)$ is small and that $(h(1+ag)^K g^{-1}) \prod_{k=1}^{K+1} v^{(k)} \pmod{q}$ is the decoded message, so its high order bits are what we want to obtain.

14.4 Witness encryption based on 3–exact cover

- 3–exact cover problem:
  A subset of $\{1, 2, \ldots, 3K\}$ which has exactly three elements is called a piece. A

collection of K pieces without intersection is called a 3–exact cover of $\{1, 2, \ldots, 3K\}$. The 3–exact cover problem is that, for randomly given $N(K)$ different pieces with a hidden 3–exact cover, find it. If $N(K) = \mathcal{O}(K)$, it easy. If $N(K) = \mathcal{O}(K^2)$, it is hard.

- Encryption:
  - Sample short elements $v^{(1)} \cdots v^{(3K)} \in R$.
  - Compute $v^{(1)} \cdots v^{(3K)} y^K p_{zt} \pmod q$.
  - Then EKEY is its high-order bits.
    Hide EKEY into pieces as follows. Randomly generate $N(K)$ different pieces of $\{1, 2, \ldots, 3K\}$ with a hidden 3–exact cover called EC. For each piece $\{i_1, i_2, i_3\}$, compute noised encoding of $v^{(i_1)} v^{(i_2)} v^{(i_3)}$, i.e.,

$$\begin{aligned} V^{\{i_1,i_2,i_3\}} &= v^{(i_1)} v^{(i_2)} v^{(i_3)} y + (u^{(\{i_1,i_2,i_3\},1)} x^{(1)} \\ &\quad + u^{(\{i_1,i_2,i_3\},2)} x^{(2)}) \pmod q. \end{aligned} \tag{14.18}$$

- Decryption: If one knows EC, compute $p_{zt} \prod_{\{i_1,i_2,i_3\} \in EC} V^{(i_1,i_2,i_3)} \pmod q$. Then EKEY is its high-order bits.

14.5 Breaking WE based on the hardness of 3–exact cover problem

Given $N(K) = \mathcal{O}(K^2)$ different pieces of $\{1, 2, \ldots, 3K\}$, $\{i_1, i_2, i_3\}$ is called a combined piece if

1. $\{i_1, i_2, i_3\}$ is not a piece given;
2. $\{i_1, i_2, i_3\} = (\{j_1, j_2, j_3\} \cup \{k_1, k_2, k_3\}) - \{l_1, l_2, l_3\}$;
3. $\{j_1, j_2, j_3\}$, $\{k_1, k_2, k_3\}$, $\{l_1, l_2, l_3\}$ are pieces given.

$\{i_1, i_2, i_3\}$ is called a second-order combined piece if

1. $\{i_1, i_2, i_3\}$ is neither a piece nor a combined piece;
2. $\{i_1, i_2, i_3\} = (\{j_1, j_2, j_3\} \cup \{k_1, k_2, k_3\}) - \{l_1, l_2, l_3\}$;
3. $\{j_1, j_2, j_3\}$, $\{k_1, k_2, k_3\}$, $\{l_1, l_2, l_3\}$ are pieces given or combined pieces.

We define combined 3–exact cover of $\{1, 2, \ldots, 3K\}$ as before.
The combined 3–exact cover problem is to "find a combined 3–exact cover among pieces, combined pieces, and second-order combined pieces."

Claim: The combined 3–exact cover problem is easy.
We are given random K^2 pieces, and there is a hidden 3–exact cover among them. Then for a random $\{i_1, i_2, i_3\}$ which is not piece,

$$\text{Prob}(\{i_1, i_2, i_3\} \text{ is not a combined piece}) \propto e^{-1},$$

as shown below. Hence, from the random K^2 pieces, we obtain about $(1-e^{-1})C_3^{3K}$ different subsets of $\{1,2,\ldots,3K\}$ which are pieces or combined pieces. There are about $e^{-1}C_3^{3K}$ left over 3-element subsets of $\{1,2,\ldots,3K\}$ which are neither pieces nor combined pieces. Choose one $\{i_1,i_2,i_3\}$ from them. We show that

$$\text{Prob}(\{i_1,i_2,i_3\} \text{ is not a second-order piece}) \propto e^{-K^3}$$

by the same method of computatiing Prob($\{i_1,i_2,i_3\}$ is not a combined piece). Hence, almost all of different C_3^{3K} subsets of $\{1,2,\ldots,3K\}$ which consists of 3 elements are pieces, combined pieces, or second-order combined pieces, so the combined 3–exact cover problem is easily solved by choosing a random 3–exact cover among pieces, combined pieces, and 2nd order combined pieces.

Computation of Prob($\{i_1,i_2,i_3\}$ is not a combined piece)

Take a random $\{i_1,i_2,i_3\}$ which is not a piece and fix it. Take a random $\{\alpha,\beta,\gamma\}$ from $\{1,2,\ldots,3K\}-\{i_1,i_2,i_3\}$. Then partition $\{\alpha,\beta,\gamma,i_1,i_2,i_3\}$ into two parts, $\{j_1,j_2,j_3\}$ and $\{k_1,k_2,k_3\}$. Let $\{l_1,l_2,l_3\}=\{\alpha,\beta,\gamma\}$. The number of possibilities of such 3-triples $\{j_1,j_2,j_3\}$, $\{k_1,k_2,k_3\}$, $\{l_1,l_2,l_3\}$ is $C_3^{3K-3}\cdot C_3^6$. Hence, the probability out of all possible 3-triples is

$$\frac{C_3^{3K-3}\cdot C_3^6}{(C_3^{3K})^3} \approx \frac{80}{81K^6} \approx \frac{1}{K^6}.$$

Hence, the probability that there is no 3 triples $\{j_1,j_2,j_3\}$, $\{k_1,k_2,k_3\}$, $\{l_1,l_2,l_3\}$ such that

$$\{j_1,j_2,j_3\}\cup\{k_1,k_2,k_3\}\supset\{i_1,i_2,i_3\}$$
$$\{l_1,l_2,l_3\}=\{j_1,j_2,j_3\}\cup\{k_1,k_2,k_3\}-\{i_1,i_2,i_3\}$$

among 3 random pieces $\{j_1,j_2,j_3\},\{k_1,k_2,k_3\},\{l_1,l_2,l_3\}$ is about

$$\left(1-\frac{1}{K^6}\right)^{\mathcal{O}(K^2)(\mathcal{O}(K^2)-1)(\mathcal{O}(K^2)-2)} \approx \exp\left(-\frac{\mathcal{O}(K^2)^3}{K^6}\right) \approx e^{-1}.$$

Take a fixed combined 3–exact cover. Take an element $\{i_1,i_2,i_3\}$ of this combined 3–exact cover.

1. If $\{i_1,i_2,i_3\}$ is a piece, we count $+1$.
2. If $\{i_1,i_2,i_3\}$ is a combined piece, so that

   $$\{i_1,i_2,i_3\}=\{j_1,j_2,j_3\}\cup\{k_1,k_2,k_3\}-\{l_1,l_2,l_3\},$$

   count $\{i_1,i_2,i_3\}\to+1$, $\{k_1,k_2,k_3\}\to+1$, $\{l_1,l_2,l_3\}\to-1$.
3. If $\{i_1,i_2,i_3\}$ is a second-order combined piece, then

   $$\{i_1,i_2,i_3\}=\{j_1,j_2,j_3\}\cup\{k_1,k_2,k_3\}-\{l_1,l_2,l_3\},$$

   where $\{i_1,i_2,i_3\}$, $\{k_1,k_2,k_3\}$, $\{l_1,l_2,l_3\}$ are pieces given or combined pieces.

(3–1) If $\{i_1,i_2,i_3\}$ is a piece given, count $+1$.
If $\{i_1,i_2,i_3\}$ is a combined piece, count

$$\begin{array}{ccccccc}\{i_1,i_2,i_3\} & = & \{\alpha_1,\alpha_2,\alpha_3\} & \cup & \{\beta_1,\beta_2,\beta_3\} & - & \{\gamma_1,\gamma_2,\gamma_3\}. \\ & & +1 & & +1 & & -1\end{array}$$

(3–2) Similarly for $\{k_1, k_2, k_3\}$.

(3–3) If $\{l_1, l_2, l_3\}$ is a piece given, count -1.
If $\{l_1, l_2, l_3\}$ is a combined piece, count

$$\{l_1, l_2, l_3\} = \underset{-1}{\{\epsilon_1, \epsilon_2, \epsilon_3\}} \cup \underset{-1}{\{\delta_1, \delta_2, \delta_3\}} - \underset{+1}{\{\xi_1, \xi_2, \xi_3\}}.$$

Note: It is possible that one piece is counted several times.

$$\begin{aligned} CPF &= \text{collection of all positive factors} \\ NPF &= \text{the number of positive factors} \end{aligned}$$

CNF and NNF are similarly defined.

Remark 14.5.1. $NPF - NNF = K$.

Since there are about K^2 pieces with factors $(+1)$, there are $(1 - e^{-2})C_3^{3K} - K^2$ combined pieces with factors $(+, +, -)$, and $e^{-2}C_3^{3K}$ second-order combined pieces with factors at most $(+ + + + +, - - - -)$. Hence, for a randomly chosen combined 3–exact cover, it is almost certain that $NPF \le 3K$, hence $NNF \le 2K$.

$$(\because 5e^{-2} + 2 \cdot \left(1 - e^{-2} \cdot \frac{K^2}{C_3^{3K}}\right) + 1 \cdot \frac{K^2}{C_3^{3K}} \le 2 + 3e^{-2} < 3)$$

If all of our combined 3–exact cover consists of pure pieces, $NPF - NNF = NPF = K$. If one of pure pieces is replaced by a combined piece, $NPF - NNF$ is not changed. The same result holds for second-order combined pieces.

Breaking WE

Randomly take a combined 3–exact cover $\to$ Obtain CPF and CNF.
For a positive factor $(pf) = \{i_1, i_2, i_3\}$, denote the secret of (pf) as $v^{(pf)} = v^{(i_1)}v^{(i_2)}v^{(i_3)}$, and the equivalent secret of $v(pf)$ as $v'^{(pf)}$.

$$PPF := \prod_{pf \in CPF} v'^{(pf)} \tag{14.19}$$

$$PNF := \prod_{nf \in CNF} v'^{(nf)} \tag{14.20}$$

$$PTS := \prod_{k=1}^{3K} v^{(k)} \tag{14.21}$$

Then

1. $\displaystyle\prod_{pf \in CPF} v^{(pf)} = PTS \times \prod_{nf \in CNF} v^{(nf)}$

2. $\displaystyle PPF - \prod_{pf \in CPF} v^{(pf)} \in \langle g \rangle$

3. $\displaystyle PNF - \prod_{nf \in CNF} v^{(nf)} \in \langle g \rangle$

4. $PPF - PNF \times PTS \in \langle g \rangle$

If PTS' is an equivalent secret of PTS, then $PPF - PNF \times PTS' \in \langle g \rangle$, since $PTS' - PTS \in \langle g \rangle$. Conversely, if PNF and g are coprime, and if $PPF - PNF \times PTS' \in \langle g \rangle$, then PTS' is an equivalent secret of PTS, since in this case $PNF \times (PTS' - PTS) \in \langle g \rangle$ implies $(PTS' - PTS) \in \langle g \rangle$.

Note that the Hermite normal form of

$$g = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-1} \\ -g_{n-1} & g_0 & \cdots & g_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ -g_1 & -g_2 & \cdots & g_0 \end{pmatrix}, \tag{14.22}$$

which is the matrix representation of $(g, xg, \ldots, x^{n-1}g)^T$, is

$$G = \begin{pmatrix} G_0 & & & \\ G_1 & 1 & & \\ \vdots & & \ddots & \\ G_{n-1} & & & 1 \end{pmatrix}, \tag{14.23}$$

where G_0 is the absolute value of $\det g$, and $G_i (\text{mod } G_0) = G_i$. This can be obtained by Gauss elimination once the basis of $\langle g \rangle$ is formed. Hence,

$$\begin{aligned} & PPF - PNF \times PTS' \in \langle g \rangle & (14.24) \\ \Leftrightarrow \; & PPF\ G^{-1} - PTS' \times \overline{PNF} \times G^{-1} \in R, & (14.25) \end{aligned}$$

where

$$\overline{PNF} = \begin{pmatrix} PNF_0 & PNF_1 & \cdots & PNF_{n-1} \\ -PNF_{n-1} & PNF_0 & \cdots & PNF_{n-2} \\ \vdots & & \ddots & \vdots \\ -PNF_1 & -PNF_2 & \cdots & PNF_0 \end{pmatrix}. \tag{14.26}$$

Let lcm be the least common multiple of all denominators of the entries of $PPF\ G^{-1}$ and $\overline{PNF} \times G^{-1}$. Then

$$\begin{aligned} & (lcm \times PPF \times G^{-1}) \ (\text{mod } lcm) & (14.27) \\ & = PTS' \times (lcm \overline{PNF} \times G^{-1}) \ (\text{mod } lcm). & (14.28) \end{aligned}$$

Note that there is at least one solution, namely PTS, which we do not know. Obtain a solution PTS'. Let $\eta = PTS'$, and compute $\eta' = Y\eta$. Let $\eta'' = \eta' (\text{mod } X^{(1)})$, and again compute $\eta''' = y(x^{(1)})^{-1}\eta'' (\text{mod } q)$. The high-order bits of η''' is then what we wanted.

Remark 14.5.2. We must obtain the Hermite normal form of $\langle g \rangle$ for an unknown small g, when Y, $X^{(1)}$, $X^{(2)}$ are public. First we obtain the Hermite normal forms of $\left\langle h(1+ag)^{K-2} b^{(1)} \right\rangle$ and $\left\langle h(1+ag)^{K-2} b^{(1)} g \right\rangle$ when the principal ideals $\langle Y \rangle$, $\left\langle X^{(1)} \right\rangle$, $\left\langle X^{(2)} \right\rangle$ are known. Note that if the Hermite normal form of the principal ideal $\langle g' \rangle$ is

$$\begin{pmatrix} G'_0 & & & \\ G'_1 & 1 & & \\ \vdots & & \ddots & \\ G'_{n-1} & & & 1 \end{pmatrix}$$

and g is a factor g', then the Hermite normal form of $\langle g \rangle$ is

$$\begin{pmatrix} G_0 & & & \\ G_1' (\text{mod } G_0) & 1 & & \\ \vdots & & \ddots & \\ G_{n-1}' (\text{mod } G_0) & & & 1 \end{pmatrix},$$

where G_0 is the determinant of $\langle g \rangle$.

14.6 Computing the Hermite Normal Form of $\langle g \rangle$ by computing the Hermite Normal Forms of $\left\langle h(1+ag)^{K-2} b^{(1)} \right\rangle$ and $\left\langle h(1+ag)^{K-2} b^{(1)} g \right\rangle$

We assume that $1 + ag$ and $b^{(1)} g$ are coprime.

1. Gaussian sample Z from the lattice $\langle Y \rangle$.

2. Compute $Z' = Z \mod X^{(1)}$. Then Z' is uniformly distributed over the intersection area $\left\langle h(1+ag)^{K-2} b^{(1)} \right\rangle \cap PP(X^{(1)})$. (Since $1 + ag$ and $b^{(1)} g$ are coprime, multiplication (or division) by $1 + ag$ preserves the uniformity over $PP(X^{(1)})$.)

3. Compute the determinant of $\langle Z' \rangle$.

4. Repeat the above steps several times.

5. Compute the greatest common divisor of the polynomially many sample. Then with a high probability, it is the determinant of $\left\langle h(1+ag)^{K-2} b^{(1)} \right\rangle$. Hence, we obtain the Hermite normal form of $\left\langle h(1+ag)^{K-2} b^{(1)} \right\rangle$ from that of $\langle Y \rangle$. Z' is of the form $\langle Y \rangle - \left\langle X^{(1)} \right\rangle$, so Z' is in the greatest common divisor of $\langle Y \rangle$ and $\left\langle X^{(1)} \right\rangle$, which is $\left\langle h(1+ag)^{K-2} b^{(1)} \right\rangle$, and of course in the parallelepiped $PP(X^{(1)})$.

Similarly, we obtain the Hermite normal form of $\left\langle h(1+ag)^{K-2} b^{(1)} g \right\rangle$ by sampling from the lattice $\left\langle X^{(2)} \right\rangle$. Then compute $\mod X^{(1)}, \ldots$

With the two Hermite normal forms of $\left\langle h(1+ag)^{K-2} b^{(1)} \right\rangle$ and $\left\langle h(1+ag)^{K-2} b^{(1)} g \right\rangle$, we obtain the Hermite normal form of $\langle g \rangle$. (Just divide the determinant of $\left\langle h(1+ag)^{K-2} b^{(1)} g \right\rangle$ by the determinant of $\left\langle h(1+ag)^{K-2} b^{(1)} \right\rangle$, then obtain the determinant of $\langle g \rangle$.)

Remark 14.6.1. Recently a quantum algorithm was found that can compute small generators of principal ideals in the cyclotomic ring. (In particular, Soliloquy; Campbell, Groves, Shepherd. [Cam14]) That is, small generators themselves of $\langle g \rangle$ are found, not only the secrets of multipartite NIKE or WE. But the cryptanalysis of Hu and Jia are classical analysis.

Appendix A

Hermite Normal Form of Ideal Lattices (following Ding and Lindner, Smart and Vercauteren)

Let $I \subseteq R = \mathbb{Z}[x]/\langle f(x) \rangle$ be an ideal, where $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ is an irreducible monic polynomial. Let L be the corresponding ideal lattice under the coefficient embedding, and $B \in \mathbb{Z}^{n \times n}$ a basis of L. Then we have

$$\begin{pmatrix} 0 \;\; 0 \;\; \cdots \;\; 0 & -a_0 \\ & \vdots \\ I_{n-1} & -a_{n-1} \end{pmatrix} B = BT$$

for some integral matrix T, because it corresponds to the invariance of I under the multiplication by x. If B is the HNF-basis of L, then the diagonal entries form a division chain

$$B_{(n,n)} \mid B_{(n-1,n-1)} \mid \cdots \mid B_{(1,1)},$$

because when the ith column $\begin{pmatrix} * \\ B_{(i,i)} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ is multiplied by x, it becomes $\begin{pmatrix} 0 \\ * \\ B_{(i,i)} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, and it should be a linear combination of B over integers, i.e., $\begin{pmatrix} 0 \\ * \\ B_{(i,i)} \\ 0 \\ \vdots \\ 0 \end{pmatrix} = B\mathbf{t}$ for some integral vector $\mathbf{t}$. Comparing both sides, especially the $(i+1)$th component, we have $B_{(i+1,i+1)}\mathbf{t}_{i+1} = B_{(i,i)}$, showing that $B_{(i+1,i+1)} \mid B_{(i,i)}$.

When $I = \langle p, x - \alpha \rangle$, two element representation of I, where p is the norm of I and α is a root of $f(x)$ modulo p, the corresponding HNF representation is very simple. Since

$$p, px, \ldots, px^{n-1}, (x-\alpha), x(x-\alpha), \ldots, x^2(x-\alpha), \ldots, x^{n-1}(x-\alpha)$$

are all in the ideal I and span I, we obtain HNF of the ideal lattice L,

$$\begin{pmatrix} p & -\alpha & -\alpha^2 & \cdots & -\alpha^{n-1} \\ 0 & & & & \\ 0 & & & & \\ \vdots & & I_{n-1} & & \\ 0 & & & & \end{pmatrix},$$

where all integers in the first row, and in the second column and onward, are taken modulo p. But it is a bad basis of ideal lattice I, in general.

Appendix B

Notes on Cyclotomic Fields with Examples (by H. Kim)

B.1 Cyclotomic Number Fields & Ring of Integers

The group of units For $m = 2^{k+1}$, the group of units in $\mathbb{Z}_m$ is given by

$$\mathbb{Z}_m^* = \left\{1, 3, 5, 7, 9, \ldots, 2^{k+1} - 1\right\},$$

so $n := \varphi(m) = |\mathbb{Z}_m^*| = 2^k$.

Cyclotomic number fields & ring of integers The minimal polynomial over $\mathbb{Q}$ of a primitive mth root of unity is called the mth *cyclotomic polynomial*, and it is denoted by $\Phi_m(x)$. Since $\Phi_m(x) \mid x^m - 1$, the coefficients of $\Phi_m(x)$ are in $\mathbb{Z}$ by Gauss's Lemma, i.e., $\Phi_m(x) \in \mathbb{Z}[x]$.

When $m = 2^{k+1}$, it is given by

$$\Phi_m(x) = x^{2^k} + 1,$$

so the field extension of $\mathbb{Q}$ by an mth root of unity is

$$\mathbb{Q}(\zeta_m) = \mathbb{Q}[x]/\Phi_m(x) = \mathbb{Q}[x]/(x^{2^k} + 1).$$

$\mathbb{Q}(\zeta_m)$ is therefore a degree 2^k field extension over $\mathbb{Q}$, and $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{2^k-1}$ is a $\mathbb{Q}$-basis.

An element of $\mathbb{Q}(\zeta_m)$ is said to be *integral* (over $\mathbb{Z}$) if it is the root of a monic polynomial with integer coefficients. For example, ζ_m is integral since it is the root of the polynomial $x^m - 1$. The *ring of integers* for $\mathbb{Q}(\zeta_m)$, i.e., the set of integral elements of $\mathbb{Q}(\zeta_m)$, is given by

$$R := \mathbb{Z}[\zeta_m] = \mathbb{Z}[x]/\Phi_m(x) = \mathbb{Z}[x]/(x^{2^k} + 1).$$

R is a Dedekind domain, and a free abelian group of rank 2^k. Any $\mathbb{Z}$-basis of R is a $\mathbb{Q}$-basis of $\mathbb{Q}(\zeta_m)$, since linear independence over $\mathbb{Z}$ is equivalent to linear independence over $\mathbb{Q}$. Any $\mathbb{Z}$-basis of R is called an *integral basis*. $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{2^k-1} \in R$ is an integral basis, called the *power basis*. Note that $\mathbb{Q}(\zeta_m)$ is a field of fractions for R. Since R is a Dedekind domain, every nonzero ideal of R can be written uniquely as a product of prime ideals.

Examples

- $m = 4$
  - $\mathbb{Z}_m^* = \{1, 3\}$
  - $n = 2$
  - $\mathbb{Q}(\zeta_m) = \mathbb{Q}[x]/(x^2+1) = \mathbb{Q}(i)$
  - $R = \mathbb{Z}[x]/(x^2+1) = \mathbb{Z}[i]$
  - Power basis: $\{1, i\}$
- $m = 8$
  - $\mathbb{Z}_m^* = \{1, 3, 5, 7\}$
  - $n = 4$
  - $\mathbb{Q}(\zeta_m) = \mathbb{Q}[x]/(x^4+1) = \mathbb{Q}\left(\frac{1+i}{\sqrt{2}}\right)$
  - $R = \mathbb{Z}[x]/(x^4+1) = \mathbb{Z}\left[\frac{1+i}{\sqrt{2}}\right]$
  - Power basis: $\left\{1, \frac{1+i}{\sqrt{2}}, i, \frac{-1+i}{\sqrt{2}}\right\}$

Note that $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_4) \subseteq \mathbb{Q}(\zeta_8)$. This is because ζ_8^2 is a 4th root of unity. (For example, $\left(\frac{1+i}{\sqrt{2}}\right)^2 = i$.) More generally, if $m' \mid m$, then $\zeta_m^{m/m'}$ is an m'th root of unity, so $\mathbb{Q}(\zeta'_m) \subseteq \mathbb{Q}(\zeta_m)$. If $m = \prod_\ell m_\ell$ is a prime power factorization, i.e., the m_ℓ are powers of distinct primes, then $\mathbb{Q}(\zeta_{m_\ell}) \subseteq \mathbb{Q}(\zeta_m)$, and there is an isomorphism

$$\bigotimes_\ell \mathbb{Q}(\zeta_{m_\ell}) \xrightarrow{\sim} \mathbb{Q}(\zeta_m)$$

such that $\otimes_\ell a_\ell \mapsto \prod_\ell a_\ell$. For example, $72 = 2^3 3^2$, so $\mathbb{Q}(\zeta_{2^3}) \otimes \mathbb{Q}(\zeta_{3^2}) \xrightarrow{\sim} \mathbb{Q}(\zeta_{72})$ via $a \otimes b \mapsto ab$. The inclusion $\mathbb{Z}[\zeta_{m_\ell}] \hookrightarrow \mathbb{Q}(\zeta_{m_\ell})$ induces an injective[1] ring homomorphism

$$\bigotimes_\ell \mathbb{Z}[\zeta_{m_\ell}] \hookrightarrow \bigotimes_\ell \mathbb{Q}(\zeta_{m_\ell}),$$

which can be shown to be integral. Hence, $\bigotimes_\ell \mathbb{Z}[\zeta_{m_\ell}] \xrightarrow{\sim} \mathbb{Z}[\zeta_m]$.

B.2 The Space H and the Canonical Embedding

B.2.1 The Space H

$\mathbb{C}^{\mathbb{Z}_m^*}$ denotes the set of all functions $\mathbb{Z}_m^* \to \mathbb{C}$. It has an obvious ring structure. It can be viewed as the Cartesian product $\mathbb{C}^n$ whose elements are indexed by the elements of $\mathbb{Z}_m^*$, and both addition and multiplication are component-wise.

The space H is defined by

$$H := \left\{x \in \mathbb{C}^{\mathbb{Z}_m^*} \mid x_i = \bar{x}_{m-i} \quad \forall i \in \mathbb{Z}_m^*\right\}.$$

[1] Recall that an abelian group is flat if and only if torsion-free.

$H \subseteq \mathbb{C}^{\mathbb{Z}_m^*}$ is a real subspace of dimension n. In fact, the $\mathbb{C}$-inner product on $\mathbb{C}^{\mathbb{Z}_m^*}$ induces an $\mathbb{R}$-inner product on H, and there is an $\mathbb{R}$-inner product space isomorphism $\mathbb{R}^n \xrightarrow{\sim} H$ via the n-by-n unitary matrix

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & & & & & i \\ & \ddots & & & \iddots & \\ & & 1 & i & & \\ & & 1 & -i & & \\ & \iddots & & & \ddots & \\ 1 & & & & & -i \end{pmatrix}.$$

Examples

- $m = 4: \ H = \left\{ (a + ib, a - ib) \in \mathbb{C}^{\{1,3\}} \mid a, b \in \mathbb{R} \right\} \simeq \mathbb{R}^2$ via

  $$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}.$$

  Note that $\det U = -i$.

- $m = 8: \ H = \left\{ (a + id, b + ic, b - ic, a - id) \in \mathbb{C}^{\{1,3,5,7\}} \mid a, b, c, d \in \mathbb{R} \right\} \simeq \mathbb{R}^4$ via

  $$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & i \\ 0 & 1 & i & 0 \\ 0 & 1 & -i & 0 \\ 1 & 0 & 0 & -i \end{pmatrix}.$$

  Note that $\det U = -1$.

Lattice in H By a *lattice* in H, we will mean the image of a full-rank lattice in $\mathbb{R}^n$ under the isomorphism $\mathbb{R}^n \xrightarrow{\sim} H$. Equivalently, it is the free abelian group generated by an $\mathbb{R}$-basis of H. If $L \subseteq H$ is a lattice generated by an $\mathbb{R}$-basis $b_0, \ldots, b_{n-1}$, its *determinant* is defined by

$$\det L := |\det B|,$$

where $B = [b_0 \cdots b_{n-1}]$. If $c_0, \ldots, c_{n-1} \in H$ is another $\mathbb{R}$-basis generating L, then $B = CV$ for some unimodular matrix V, so $\det L$ is independent of the choice of an $\mathbb{R}$-basis of H generating L.

B.2.2 The Canonical Embedding

Let $i \in \mathbb{Z}_m^*$, and ω_m some fixed mth root of unity. By the universal property of polynomial rings, the inclusion $\mathbb{Q} \hookrightarrow \mathbb{C}$ extends uniquely to a ring homomorphism

$$\mathbb{Q}[x] \to \mathbb{C}$$

such that $x \mapsto \omega_m^i$. The kernel is generated by the minimal polynomial of ω_m^i, which is $\Phi_m(x)$. Hence, there is an injective $\mathbb{Q}$-algebra homomorphism $\mathbb{Q}[x]/\Phi_m(x) \hookrightarrow \mathbb{C}$ such that $\bar{x} \mapsto \omega_m^i$, i.e.,

$$\sigma_i : \mathbb{Q}(\zeta_m) \hookrightarrow \mathbb{C}$$

such that $\zeta_m \mapsto \omega_m^i$. σ_i are none other that the n Galois automorphisms on $\mathbb{Q}(\zeta_m)$ fixing $\mathbb{Q}$. In particular, they are independent, up to a permutation, of the choices of ζ_m and ω_m. Since $R = \mathbb{Z}[\zeta_m]$, σ_i is also an automorphism on R fixing $\mathbb{Z}$.

The *canonical embedding* is the function

$$\sigma : \mathbb{Q}(\zeta_m) \to \mathbb{C}^{\mathbb{Z}_m^*}, \qquad a \mapsto (\sigma_i(a))_{i\in\mathbb{Z}_m^*}.$$

It is an injective $\mathbb{Q}$-algebra homomorphism. Since $\omega_m^{m-i} = \bar{\omega}_m^i$, the image of σ lies in H.

Lattice in H induced by a $\mathbb{Q}$-basis of $\mathbb{Q}(\zeta_m)$ If $x_0, \ldots, x_{n-1} \in \mathbb{Q}(\zeta_m)$ is a $\mathbb{Q}$-basis, σ may be represented by the n-by-n matrix $(\sigma_i(x_j))$. Note that the jth column of this matrix is $\sigma(x_j) \in H$. For the power basis $1, \zeta_m, \ldots, \zeta_m^{n-1}$, the matrix becomes

$$S := (\sigma_i(\zeta_m^j)).$$

Note that a different choice of ζ_m or ω_m results in a permutation of rows or columns of S. Each σ_i induces a character $\mathbb{Q}(\zeta_m)^* \to \mathbb{C}^*$, so by the independence of characters, the rows of $(\sigma_i(x_j))$ are linearly independent over $\mathbb{C}$. Hence, $\sigma(x_0), \ldots, \sigma(x_{n-1})$ generate a lattice in H with determinant $|\det \sigma_i(x_j)| \neq 0$.

It follows that if $G \subseteq \mathbb{Q}(\zeta_m)$ is a free abelian subgroup with a basis $g_0, \ldots, g_{n-1}$, then $\sigma(G)$ is a lattice in H generated by $\sigma(g_0), \ldots, \sigma(g_{n-1})$, and $\det \sigma(G) = |\det \sigma_i(g_j)| \neq 0$. In particular, $\sigma(R)$ is a lattice in H, and $\det \sigma(R) = |\det S| \neq 0$.

If $x_0, \ldots, x_{n-1} \in \mathbb{Q}(\zeta_m)$ are linearly dependent over $\mathbb{Q}$, then $\sum_j q_j x_j = 0$ for some $q_j \in \mathbb{Q}$, not all zero, and since σ_i is $\mathbb{Q}$-linear,

$$\sum_j q_j \sigma_i(x_j) = \sigma_i\left(\sum_j q_j x_j\right) = 0.$$

Hence, the columns of the matrix $(\sigma_i(x_j))$ are linearly dependent over $\mathbb{Q}$, so $\det \sigma_i(x_j) = 0$.

Note the following:

- If $x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1} \in \mathbb{Q}(\zeta_m)$ and $y_j = \sum_k M_{jk} x_k$, where $M_{jk} \in \mathbb{Q}$, then

$$\det \sigma_i(y_j) = (\det M)(\det \sigma_i(x_j)).$$

- If $x_0, \ldots, x_{n-1}, y \in \mathbb{Q}(\zeta_m)$, then

$$\det \sigma_i(y x_j) = \det \sigma_i(y)\sigma_i(x_j) = \left(\prod_i \sigma_i(y)\right) \det \sigma_i(x_j) = \mathrm{N}(y) \det \sigma_i(x_j),$$

Examples

- $m = 4$:

$$S = \begin{pmatrix} \sigma_1(1) & \sigma_1(\zeta_4) \\ \sigma_3(1) & \sigma_3(\zeta_4) \end{pmatrix} = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$$

  $\det S = -2i$, so $\det \sigma(R) = |-2i| = 2$.

- $m = 8$:

$$S = \begin{pmatrix} \sigma_1(1) & \sigma_1(\zeta_8) & \sigma_1(\zeta_8^2) & \sigma_1(\zeta_8^3) \\ \sigma_3(1) & \sigma_3(\zeta_8) & \sigma_3(\zeta_8^2) & \sigma_3(\zeta_8^3) \\ \sigma_5(1) & \sigma_5(\zeta_8) & \sigma_5(\zeta_8^2) & \sigma_5(\zeta_8^3) \\ \sigma_7(1) & \sigma_7(\zeta_8) & \sigma_7(\zeta_8^2) & \sigma_7(\zeta_8^3) \end{pmatrix} = \begin{pmatrix} 1 & \zeta_8 & \zeta_8^2 & \zeta_8^3 \\ 1 & \zeta_8^3 & -\zeta_8^2 & \zeta_8 \\ 1 & -\zeta_8 & \zeta_8^2 & -\zeta_8^3 \\ 1 & -\zeta_8^3 & -\zeta_8^2 & -\zeta_8 \end{pmatrix}$$

  $\det S = -16$, so $\det \sigma(R) = |-16| = 16$.

Trace and norm For $a \in \mathbb{Q}(\zeta_m)$, define

$$\operatorname{Tr}(a) := \sum_{i \in \mathbb{Z}_m^*} \sigma_i(a), \qquad \operatorname{N}(a) := \prod_{i \in \mathbb{Z}_m^*} \sigma_i(a).$$

Note that if $a \in R$, then $\operatorname{Tr}(a) \in R$ and $\operatorname{N}(a) \in R$.

Note the following:

- $\operatorname{Tr}(a)$ and $\operatorname{N}(a)$ are independent of the choices of ζ_m and ω_m.
- $\operatorname{Tr}(1) = n$ and $\operatorname{N}(1) = 1$.
- Tr is $\mathbb{Q}$-linear.
- $\operatorname{N}(ab) = \operatorname{N}(a)\operatorname{N}(b)$ for all $a, b \in \mathbb{Q}(\zeta_m)$. Hence, if $u \in R$ is a unit, then $\operatorname{N}(u) = \pm 1$. (The converse is also true; see Corollary B.2.3.)
- For all $a \in \mathbb{Q}(\zeta_m)$, $\operatorname{N}(a) = 0$ if and only if $a = 0$.

Proposition B.2.1. Let $a \in \mathbb{Q}(\zeta_m)$, and A an n-by-n matrix with entries in $\mathbb{Q}$ representing the multiplication map $\mathbb{Q}(\zeta_m) \xrightarrow{a} \mathbb{Q}(\zeta_m)$ with respect to some $\mathbb{Q}$-basis. Then $\operatorname{Tr} A = \operatorname{Tr}(a)$ and $\det A = \operatorname{N}(a)$.

Proof. Let $f = \det(xI - A)$ be the characteristic polynomial. Then clearly

$$f = x^n - (\operatorname{Tr} A)x^{n-1} + \cdots + (-1)^n \det A. \tag{B.1}$$

By the Cayley-Hamilton theorem, a is a root of f, so f is divisible by the minimal polynomial of a. In fact, it is easy to show that if $m_a \in \mathbb{Q}[x]$ is the minimal polynomial of a with degree d, then $f = m_a^{n/d}$.

Let $a_0, \ldots, a_{d-1} \in \mathbb{Q}(\zeta_m)$ be the roots of m_a (they all lie in $\mathbb{Q}(\zeta_m)$ since $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_m)$ is a splitting field extension of Φ_m, hence normal), so that $m_a = (x - a_0) \cdots (x - a_{d-1})$. Then

$$m_a^{n/d} = x^n - \frac{n}{d}\sum_i a_i x^{n-1} + \cdots + (-1)^n \left(\prod_i a_i\right)^{n/d},$$

so comparing with (B.1), we see that

$$\operatorname{Tr} A = \frac{n}{d}\sum_i a_i, \qquad \det A = \left(\prod_i a_i\right)^{n/d}. \tag{B.2}$$

Now consider the extensions

$$\mathbb{Q} \overset{d}{\subseteq} \mathbb{Q}(a) \overset{n/d}{\subseteq} \mathbb{Q}(\zeta_m).$$

Being separable, $a_0, \ldots, a_{d-1} \in \mathbb{Q}(\zeta_m)$ are distinct, and there are exactly d embeddings of $\mathbb{Q}(a)$ into $\mathbb{Q}(\zeta_m)$ fixing $\mathbb{Q}$ (corresponding to $a \mapsto a_i$), each of which extends to exactly n/d automorphisms ($\mathbb{Q} \subseteq \mathbb{Q}(\zeta_m)$ being normal) of $\mathbb{Q}(\zeta_m)$ fixing $\mathbb{Q}$. It follows that

$$\sum_{i \in \mathbb{Z}_m^*} \sigma_i(a) = \frac{n}{d}\sum_i a_i, \qquad \prod_{i \in \mathbb{Z}_m^*} \sigma_i(a) = \left(\prod_i a_i\right)^{n/d}.$$

By (B.2), it follows that $\operatorname{Tr}(a) = \operatorname{Tr} A$ and $\operatorname{N}(a) = \det A$. $\square$

Corollary B.2.2. i. If $a \in \mathbb{Q}(\zeta_m)$, then $\mathrm{Tr}(a) \in \mathbb{Q}$ and $\mathrm{N}(a) \in \mathbb{Q}$.

ii. If $a \in R$, then $\mathrm{Tr}(a) \in \mathbb{Z}$ and $\mathrm{N}(a) \in \mathbb{Z}$.

Proof. i is immediate from Proposition B.2.1. If $a \in R$, then

$$\mathrm{Tr}(a), \mathrm{N}(a) \in R \cap \mathbb{Q} = \mathbb{Z},$$

since $\mathbb{Z}$ is integrally closed.

Alternatively, any $\mathbb{Z}$-basis of R is a $\mathbb{Q}$-basis of $\mathbb{Q}(\zeta_m)$, and with respect to this basis, the multiplication maps $\mathbb{Q}(\zeta_m) \xrightarrow{r} \mathbb{Q}(\zeta_m)$ and $R \xrightarrow{r} R$ by $r \in R$ are represented by the same matrix A with integer entries, whoses trace and determinant are integers. □

Corollary B.2.3. For all $r \in R$, $\mathrm{N}(r) = \pm 1$ if and only if r is a unit in R.

Proof. Any $\mathbb{Z}$-basis of R is a $\mathbb{Q}$-basis of $\mathbb{Q}(\zeta_m)$, and with respect to this basis, the multiplication maps $\mathbb{Q}(\zeta_m) \xrightarrow{r} \mathbb{Q}(\zeta_m)$ and $\varphi : R \xrightarrow{r} R$ are represented by the same matrix A with integer entries. Now r is a unit in R if and only if φ is an isomorphism if and only if $\det A \in \mathbb{Z}$ is a unit, i.e., $\det A = \pm 1$. Since $\det A = \mathrm{N}(r)$, the result follows. □

Proposition B.2.4. If $x_0, \ldots, x_{n-1} \in \mathbb{Q}(\zeta_m)$, then $\det \mathrm{Tr}(x_i x_j) = (\det \sigma_i(x_j))^2$.

Proof.

$$\mathrm{Tr}(x_i x_j) = \sum_{k \in \mathbb{Z}_m^*} \sigma_k(x_i x_j) = \sum_{k \in \mathbb{Z}_m^*} \sigma_k(x_i)\sigma_k(x_j) = (A^T A)_{ij},$$

where A is the matrix $(\sigma_i(x_j))$. Hence, $\det \mathrm{Tr}(x_i x_j) = (\det A)^2$. □

Remark B.2.5. Note that If $x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1} \in \mathbb{Q}(\zeta_m)$ and $y_j = \sum_k M_{jk} x_k$, where $M_{jk} \in \mathbb{Q}$, then

$$\det \mathrm{Tr}(y_i y_j) = (\det M)^2 \det \mathrm{Tr}(x_i x_j).$$

Corollary B.2.6. If $b_0, \ldots, b_{n-1}$ is a basis of a free abelian subgroup $G \subseteq \mathbb{Q}(\zeta_m)$, then

$$\det \sigma(G) = |\det \mathrm{Tr}(b_i b_j)|.$$

Corollary B.2.7. i. If $x_0, \ldots, x_{n-1} \in \mathbb{Q}(\zeta_m)$, then $(\det \sigma_i(x_j))^2 \in \mathbb{Q}$.

ii. If $r_0, \ldots, r_{n-1} \in R$, then $(\det \sigma_i(r_j))^2 \in \mathbb{Z}$. In particular, $(\det S)^2 \in \mathbb{Z}$.

Corollary B.2.8. $x_0, \ldots, x_{n-1} \in \mathbb{Q}(\zeta_m)$ is a $\mathbb{Q}$-basis if and only if $\det \mathrm{Tr}(x_i x_j) \neq 0$.

Examples

- $m = 4$: If $\omega_4 = i$, then

$$\begin{array}{rcl} \sigma : \mathbb{Q}(\zeta_4) & \to & \mathbb{C}^{\{1,3\}}, \\ q_0 + q_1\zeta_4 & \mapsto & (q_0 + iq, q_0 - iq_1) \end{array}$$

where $q_0, q_1 \in \mathbb{Q}$. Hence,

$$\mathrm{Tr}(q_0 + q_1\zeta_4) = 2q_0 \in \mathbb{Q},$$

$$\mathrm{N}(q_0 + q_1\zeta_4) = q_0^2 + q_1^2 \in \mathbb{Q}.$$

Since $\zeta_4^2 = -1$,

$$(p_0 + p_1\zeta_4)(q_0 + q_1\zeta_4) = p_0q_0 - p_1q_1 + (p_0q_1 + p_1q_0)\zeta_4,$$

where $p_0, p_1, q_0, q_1 \in \mathbb{Q}$. Hence, in terms of the basis $1, \zeta_4$, the multiplication map

$$\mathbb{Q}(\zeta_4) \xrightarrow{q_0+q_1\zeta_4} \mathbb{Q}(\zeta_4)$$

is represented by the matrix

$$A = \begin{pmatrix} q_0 & -q_1 \\ q_1 & q_0 \end{pmatrix}.$$

Note that

$$\begin{aligned} \operatorname{Tr} A &= 2q_0 = \operatorname{Tr}(q_0 + q_1\zeta_4), \\ \det A &= q_0^2 + q_1^2 = \mathrm{N}(q_0 + q_1\zeta_4). \end{aligned}$$

- $m = 8$: If $\omega_8 = \frac{1+i}{\sqrt{2}}$, then

$$\begin{aligned} \sigma : \mathbb{Q}(\zeta_8) &\to \mathbb{C}^{\{1,3,5,7\}}, \\ q_0 + q_1\zeta_8 + q_2\zeta_8^2 + q_3\zeta_8^3 &\mapsto (q_0 + q_1\zeta_8 + q_2\zeta_8^2 + q_3\zeta_8^3, \\ &\quad\;\; q_0 + q_3\zeta_8 - q_2\zeta_8^2 + q_1\zeta_8^3, \\ &\quad\;\; q_0 - q_1\zeta_8 + q_2\zeta_8^2 - q_3\zeta_8^3, \\ &\quad\;\; q_0 - q_3\zeta_8 - q_2\zeta_8^2 - q_1\zeta_8^3) \end{aligned}$$

where $q_0, q_1, q_2, q_3 \in \mathbb{Q}$. Hence,

$$\operatorname{Tr}(q_0 + q_1\zeta_8 + q_2\zeta_8^2 + q_3\zeta_8^3) = 4q_0 \in \mathbb{Q},$$

and after some calculation, one can verify that

$$\mathrm{N}(q_0 + q_1\zeta_8 + q_2\zeta_8^2 + \zeta_8^3) = (q_0^2 - q_2^2 + 2q_1q_3)^2 + (q_1^2 - q_3^2 - 2q_0q_2)^2 \in \mathbb{Q}.$$

It is easy to see that in terms of the basis $1, \zeta_8, \zeta_8^2, \zeta_8^3$, the multiplication map

$$\mathbb{Q}(\zeta_8) \xrightarrow{q_0+q_1\zeta_8+q_2\zeta_8^2+q_3\zeta_8^3} \mathbb{Q}(\zeta_8)$$

is represented by the *anti-circulant* matrix

$$A = \begin{pmatrix} q_0 & -q_3 & -q_2 & -q_1 \\ q_1 & q_0 & -q_3 & -q_2 \\ q_2 & q_1 & q_0 & -q_3 \\ q_3 & q_2 & q_1 & q_0 \end{pmatrix}.$$

Note that

$$\operatorname{Tr} A = 4q_0 = \operatorname{Tr}(q_0 + q_1\zeta_8 + q_2\zeta_8^2 + q_3\zeta_8^3).$$

One can also verify that

$$\det A = \mathrm{N}(q_0 + q_1\zeta_8 + q_2\zeta_8^2 + q_3\zeta_8^3).$$

B.3 Discriminant

The *discriminant* of $\mathbb{Q}(\zeta_m)$ is defined by

$$\Delta_{\mathbb{Q}(\zeta_m)} := (\det \sigma(R))^2.$$

Hence, if $b_0, \ldots, b_{n-1} \in R$ is any integral basis, then

$$\Delta_{\mathbb{Q}(\zeta_m)} = |\det \sigma_i(b_j)|^2 = |\det \mathrm{Tr}(b_i b_j)|.$$

In particular,

$$\Delta_{\mathbb{Q}(\zeta_m)} = |\det S|^2.$$

Since $(\det S)^2 \in \mathbb{Z}$ (Corollary B.2.7), $\Delta_{\mathbb{Q}(\zeta_m)}$ is a positive integer.[2]

If $x_0, \ldots, x_{n-1} \in \mathbb{Q}(\zeta_m)$, then $x_j = \sum_i M_{ji} b_i$ for some $M_{ji} \in \mathbb{Q}$, so (see Remark B.2.5)

$$|\det \mathrm{Tr}(x_i x_j)| = (\det M)^2 \Delta_{\mathbb{Q}(\zeta_m)}. \tag{B.3}$$

Relationship with polynomial discriminant Since $S = (\sigma_i(\zeta_m^j))$ is a Vandermonde matrix,

$$\det S = \prod_{i<j} (\sigma_i(\zeta_m) - \sigma_j(\zeta_m)) = \prod_{i<j} (\omega_m^i - \omega_m^j).$$

Hence, in terms of $\Delta_{\Phi_m} := \prod_{i<j} (\omega_m^i - \omega_m^j)^2$, we have

$$\Delta_{\mathbb{Q}(\zeta_m)} = |\Delta_{\Phi_m}|.$$

Examples

- $m = 4$: We know that $\det S = -2i$, so $\Delta_{\mathbb{Q}(\zeta_m)} = |\det S|^2 = 4$. On the other hand,

$$\begin{aligned} \mathrm{Tr}(\zeta_4^i \zeta_4^j) &= \begin{pmatrix} \mathrm{Tr}(\zeta_4^0 \zeta_4^0) & \mathrm{Tr}(\zeta_4^0 \zeta_4^1) \\ \mathrm{Tr}(\zeta_4^1 \zeta_4^0) & \mathrm{Tr}(\zeta_4^1 \zeta_4^1) \end{pmatrix} \\ &= \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(i) \\ \mathrm{Tr}(i) & \mathrm{Tr}(-1) \end{pmatrix} \\ &= \begin{pmatrix} 1+1 & i-i \\ i-i & -1-1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}, \end{aligned}$$

  so

$$\Delta_{\mathbb{Q}(\zeta_m)} = |\det \mathrm{Tr}(\zeta_4^i \zeta_4^j)| = |-4| = 4.$$

- $m = 8$: We know that $\det S = -16$, so $\Delta_{\mathbb{Q}(\zeta_m)} = |\det S|^2 = 2^8$. On the other hand,

$$\mathrm{Tr}(\zeta_8^i \zeta_8^j) = \begin{pmatrix} \mathrm{Tr}(\zeta_8^0 \zeta_8^0) & \mathrm{Tr}(\zeta_8^0 \zeta_8^1) & \mathrm{Tr}(\zeta_8^0 \zeta_8^2) & \mathrm{Tr}(\zeta_8^0 \zeta_8^3) \\ \mathrm{Tr}(\zeta_8^1 \zeta_8^0) & \mathrm{Tr}(\zeta_8^1 \zeta_8^1) & \mathrm{Tr}(\zeta_8^1 \zeta_8^2) & \mathrm{Tr}(\zeta_8^1 \zeta_8^3) \\ \mathrm{Tr}(\zeta_8^2 \zeta_8^0) & \mathrm{Tr}(\zeta_8^2 \zeta_8^1) & \mathrm{Tr}(\zeta_8^2 \zeta_8^2) & \mathrm{Tr}(\zeta_8^2 \zeta_8^3) \\ \mathrm{Tr}(\zeta_8^3 \zeta_8^0) & \mathrm{Tr}(\zeta_8^3 \zeta_8^1) & \mathrm{Tr}(\zeta_8^3 \zeta_8^2) & \mathrm{Tr}(\zeta_8^3 \zeta_8^3) \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & -4 \\ 0 & 0 & -4 & 0 \\ 0 & -4 & 0 & 0 \end{pmatrix},$$

  so

$$\Delta_{\mathbb{Q}(\zeta_m)} = |\det \mathrm{Tr}(\zeta_8^i \zeta_8^j)| = |4^4| = 2^8.$$

[2] A more standard definition of $\Delta_{\mathbb{Q}(\zeta_m)}$ is $\det S$, which can be negative.

B.4 Ideals

If $I \subseteq R$ is an ideal, define $\mathrm{N}(I) := |R/I|$. Note that $\mathrm{N}(I) \geq 1$, where equality holds if and only if $I = R$.

Proposition B.4.1. If $I \subseteq R$ is a nonzero ideal, then $\mathrm{N}(I)$ is finite.

Proof. Let $I \subseteq R$ be a nonzero ideal. Then there exists a nonzero element $a \in I$, and

$$\mathrm{N}(a) = a \prod_{\substack{i \in \mathbb{Z}_m^*, \\ \omega_m^i \neq \zeta_m}} \sigma_i(a) \neq 0.$$

Since $a \in R$, $\sigma_i(a) \in R$ for all $i \in \mathbb{Z}_m^*$, so $\prod_{\zeta_m \neq \omega_m^i} \sigma_i(a) \in R$. Since $a \in I$, it follows that $\mathrm{N}(a) \in I$. Since $a \in R$, $\mathrm{N}(a) \in \mathbb{Z}$. Now $R \simeq \mathbb{Z}^n$ as an abelian group, so $R/\mathrm{N}(a)R \simeq (\mathbb{Z}/\mathrm{N}(a)\mathbb{Z})^n$ as an abelian group. Since $\mathrm{N}(a) \neq 0$, $|(\mathbb{Z}/\mathrm{N}(a)\mathbb{Z})^n| = n\,\mathrm{N}(a) < \infty$, i.e., $|R/\mathrm{N}(a)R|$ is finite. Since $\mathrm{N}(a)R \subseteq I \subseteq R$ and $R/I \simeq (R/\mathrm{N}(a)R)/(I/\mathrm{N}(a)R)$, $|R/I|$ must be finite, too. □

Remark B.4.2. It follows that $\mathrm{N}(I)$ is a positive integer for every nonzero ideal $I \subseteq R$.

Corollary B.4.3. If $I \subseteq R$ is a nonzero ideal, then $\mathrm{N}(I) \in I$.

Proof. Let $\mathrm{N}(I) = k \in \mathbb{Z}$. Since $|R/I| = k$, for $\bar{1} \in R/I$, we must have $k \cdot \bar{1} = 0 \in R/I$, i.e., $k \in I$. □

Corollary B.4.4. Every nonzero ideal of R is a free abelian group of rank n.

Remark B.4.5. It follows that if $I \subseteq R$ is a nonzero ideal, then $\sigma(I)$ is a lattice in H.

Proposition B.4.6. If $b_1, \ldots, b_k \in R$ are linearly independent over $\mathbb{Z}$ and $r \in R$ is a nonzero element, then $rb_1, \ldots, rb_k$ are linearly independent over $\mathbb{Z}$.

Proof. Consider the equation

$$0 = c_1 r b_1 + \cdots + c_k r b_k = r(c_1 b_1 + \cdots + c_k b_k),$$

where $c_1, \ldots, c_k \in \mathbb{Z}$. In view of $R = \mathbb{Z}[x]/\Phi_m(x)$, we may represent r and b_i as polynomials in $\mathbb{Z}[x]$ of degree less than n, say $r = \bar{f}$ and $b_i = \bar{g}_i$. Then the equation above implies that $\Phi_m(x)$ divides $f(c_1 g_1 + \cdots + c_k g_k)$ in $\mathbb{Z}[x]$. Since $\Phi_m(x)$ is irreducible, it is a prime ($\mathbb{Z}[x]$ being a UFD), so it divides f or $c_1 g_1 + \cdots + c_k g_k$. Since the degrees of f and $c_1 g_1 + \cdots + c_k g_k$ are both less than n, we must have $c_1 g_1 + \cdots + c_k g_k = 0$. Then $c_1 b_1 + \cdots + c_k b_k = 0$, so $c_1 = \cdots = c_k = 0$ by the linear independence of $b_1, \ldots, b_k$. □

Corollary B.4.7. If $b_0, \ldots, b_{n-1} \in R$ is an integral basis and $r \in R$ is a nonzero element, then the ideal $\langle r \rangle \subseteq R$ is a free abelian group with a basis $rb_0, \ldots, rb_{n-1}$.

Lemma B.4.8. Let $b_0, \ldots, b_{n-1} \in R$ be an integral basis, $I \subseteq R$ a nonzero ideal with a $\mathbb{Z}$-basis $c_0, \ldots, c_{n-1}$, and $c_j = \sum_i M_{ji} b_i$, where $M_{ji} \in \mathbb{Z}$. Then

$$\mathrm{N}(I) = |\det M|.$$

Proof. There exists an integral basis $b'_0, \ldots, b'_{n-1} \in R$ such that $k_0 b'_0, \ldots, k_{n-1} b'_{n-1}$ is a $\mathbb{Z}$-basis of I for some $k_0, \ldots, k_{n-1} \in \mathbb{Z}$. Then clearly $\mathrm{N}(I) = |k_0 \cdots k_{n-1}|$, so $\mathrm{N}(I) = |\det M'|$, where M' is the n-by-n diagonal matrix with diagonal entris $k_0, \ldots, k_{n-1}$, so that $k_j b_j = \sum_i M'_{ji} b_i$. More generally, change of bases corresponds to $M' \mapsto U M' V$ for some unimodular matrices U and V, so $|\det M'|$ remains unchanged. □

Proposition B.4.9. If $I \subseteq R$ is a nonzero ideal, then

$$(\det \sigma(I))^2 = \mathrm{N}(I)^2 \Delta_{\mathbb{Q}(\zeta_m)}.$$

Proof. Let $b_0, \ldots, b_{n-1} \in R$ be an integral basis, and $c_0, \ldots, c_{n-1}$ a $\mathbb{Z}$-basis of I. Then $c_j = \sum_i M_{ji} b_i$ for some $M_{ji} \in \mathbb{Z}$, so by (B.3) and Lemma B.4.8,

$$|\det \mathrm{Tr}(c_i c_j)| = \mathrm{N}(I)^2 \Delta_{\mathbb{Q}(\zeta_m)}.$$

Hence,

$$(\det \sigma(I))^2 = |\det \sigma_i(c_j)|^2 = |\det \mathrm{Tr}(c_i c_j)| = \mathrm{N}(I)^2 \Delta_{\mathbb{Q}(\zeta_m)}.$$

□

Proposition B.4.10. If $r \in R$ is a nonzero element, then $\mathrm{N}(\langle r \rangle) = |\mathrm{N}(r)|$.

Proof. Let $b_0, \ldots, b_{n-1} \in R$ be an integral basis. By Corollary B.4.7, $r b_0, \ldots, r b_{n-1}$ is a $\mathbb{Z}$-basis of $\langle r \rangle$, so by Proposition B.4.9,

$$|\det \sigma_i(r b_j)|^2 = \mathrm{N}(\langle r \rangle)^2 \Delta_{\mathbb{Q}(\zeta_m)}. \tag{B.4}$$

On the other hand, $\det \sigma_i(r b_j) = \mathrm{N}(r) \det \sigma_i(b_j)$, so

$$|\det \sigma_i(r b_j)|^2 = \mathrm{N}(r)^2 |\det \sigma_i(b_j)|^2 = \mathrm{N}(r)^2 \Delta_{\mathbb{Q}(\zeta_m)}. \tag{B.5}$$

Since $\Delta_{\mathbb{Q}(\zeta_m)} \neq 0$, (B.4) and (B.5) gives $\mathrm{N}(\langle r \rangle) = |\mathrm{N}(r)|$. □

Remark B.4.11. Note that the equality does not hold if $r = 0$.

Lemma B.4.12. If $I \subseteq R$ is a nonzero ideal and $P \subseteq R$ is a nonzero prime ideal, then there is a ring isomorphism $I/PI \simeq R/P$.

Proof. Since R is a Dedekind domain, PI and I are distinct ideals, and there is no ideal between PI and I. Hence, I/PI is an R/P-module with no intermediate submodule, so it is generated by a single nonzero element. Since $P \subseteq R$ is a maximal ideal, this means that $I/PI \simeq R/P$. □

Proposition B.4.13. $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$ for all ideals $I, J \subseteq R$.

Proof. If $I = 0$, then $IJ = 0$, so $\mathrm{N}(IJ) = \mathrm{N}(I) = |R|$, so the equality becomes

$$|R| = |R| \cdot \mathrm{N}(J).$$

Since R is infinite and $\mathrm{N}(J) \leq |R|$, the equality does hold.

Now assume that $I \neq 0$ and $J \neq 0$. Since R is a Dedekind domain, I is a product of nonzero prime ideals. If it is an empty product, i.e., $I = R$, then the equality becomes

$\mathrm{N}(J) = 1 \cdot \mathrm{N}(J)$, which is obviously true. So we may assume that $I \neq R$, and it suffices to show that $\mathrm{N}(PJ) = \mathrm{N}(P)\,\mathrm{N}(J)$ for every nonzero prime ideal $P \subseteq R$.

From the ring isomorphism

$$\frac{R/PJ}{J/PJ} \simeq R/J,$$

we have $|R/PJ| = |J/PJ| \cdot |R/J|$, i.e., $\mathrm{N}(PJ) = |J/PJ| \cdot \mathrm{N}(J)$. (Note that all three quantities are finite by Proposition B.4.1.) By Lemma B.4.12, $|J/PJ| = |R/P| = \mathrm{N}(P)$, so $\mathrm{N}(PJ) = \mathrm{N}(P)\,\mathrm{N}(J)$, as desired. $\square$

Corollary B.4.14. If $I, J \subseteq R$ are nonzero ideals, then $|I/IJ| = \mathrm{N}(J)$.

Proof. From the ring isomorphism

$$\frac{R/IJ}{I/IJ} \simeq R/I,$$

we have $|R/IJ| = |R/I| \cdot |I/IJ|$, i.e., $\mathrm{N}(IJ) = \mathrm{N}(I) \cdot |I/IJ|$. On the other hand, $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$ by Proposition B.4.13. Since all quantities here are finite and $\mathrm{N}(I) \neq 0$, we have $|I/IJ| = \mathrm{N}(J)$. $\square$

Corollary B.4.15. Let $I \subseteq R$ be a nonzero ideal. If $\mathrm{N}(I)$ is prime, then I is a prime ideal.

Proof. If $I = R$, then $\mathrm{N}(I) = 0$ is not prime, so $I \neq R$. Hence, I is a product of at least one prime ideal. Suppose that $I = J_1 J_2$, where $J_1, J_2 \subseteq R$ are ideals. Then $\mathrm{N}(I) = \mathrm{N}(J_1)\,\mathrm{N}(J_2)$, and since $\mathrm{N}(I)$ is prime, $\mathrm{N}(J_1) = 1$ or $\mathrm{N}(J_2) = 1$, i.e., $J_1 = R$ or $J_2 = R$. This shows that I is a product of at most one prime ideal. $\square$

B.4.1 Fractional ideals

An R-submodule $I \subseteq \mathbb{Q}(\zeta_m)$ is called a *fractional ideal* of R if there exists a nonzero $d \in R$ such that $dI \subseteq R$. Note that every ideal of R is a fractional ideal. An ideal of R is sometimes called an *integral* ideal. Since every nonzero integral ideal is a free abelian group of rank n (Corollary B.4.4), so is every nonzero fractional ideal. It follows that if $I \subseteq \mathbb{Q}(\zeta_m)$ is a nonzero fractional ideal, then $\sigma(I)$ is a lattice in H.

Note the following:

- If $I \subseteq \mathbb{Q}(\zeta_m)$ is a fractional ideal such that $dI \subseteq R$ for some nonzero $d \in R$, then $b_0, \ldots, b_{n-1}$ is a $\mathbb{Z}$-basis of I if and only if $db_0, \ldots, db_{n-1}$ is a $\mathbb{Z}$-basis of the integral ideal dI.
- Since $\mathbb{Q}(\zeta_m)$ is a field of fractions for R, every finitely generated R-submodule of $\mathbb{Q}(\zeta_m)$ is a fractional ideal of R. In particular, every principal R-submodule of $\mathbb{Q}(\zeta_m)$ is a fractional ideal.
- If $I, J \subseteq \mathbb{Q}(\zeta_m)$ are fractional ideals, then so are $I + J$ and IJ.

The *norm* of a nonzero fractional ideal $I \subseteq \mathbb{Q}(\zeta_m)$ is defined by

$$\mathrm{N}(I) := \mathrm{N}(dI)/|\,\mathrm{N}(d)| \in \mathbb{Q},$$

where $d \in R$ is a nonzero element such that $dI \subseteq R$. This is well-defined: if $e \in R$ is another nonzero element such that $eI \subseteq R$, then by Proposition B.4.10 and Proposition B.4.13,

$$|\operatorname{N}(e)| \operatorname{N}(dI) = \operatorname{N}(\langle e \rangle) \operatorname{N}(dI) = \operatorname{N}(edI) = \operatorname{N}(deI) = \operatorname{N}(\langle d \rangle) \operatorname{N}(eI) = |\operatorname{N}(d)| \operatorname{N}(eI).$$

For nonzero integral ideals, this definition of norm agrees with the earlier definition of norm. Note that the norm of a nonzero fractional ideal is a positive rational number.

Proposition B.4.16. Let $I \subseteq \mathbb{Q}(\zeta_m)$ be any subset. TFAE:

i. I is a nonzero fractional ideal of R.

ii. There exists $d \in R$ such that dI is a nonzero ideal of R.

Proof. i⇒ii: By definition, there exists a nonzero $d \in R$ such that $dI \subseteq R$. Since $I \subseteq \mathbb{Q}(\zeta_m)$ is an R-submodule, so is dI, i.e., $dI \subseteq R$ is an ideal. Since $d \neq 0$ and $I \neq 0$, $dI \neq 0$

i⇐ii: Since $dI \subseteq R$ is a nonzero ideal by assumption, $d \neq 0$ and $I \neq 0$. Hence, all we have to show is that $I \subseteq \mathbb{Q}(\zeta_m)$ is an R-submodule. First note that since $dI \subseteq R$ is an ideal, $I \neq \varnothing$.

- Let $i_1, i_2 \in I$. Since dI is an abelian group, $di_1 + di_2 \in dI$, i.e., $d(i_1 + i_2) \in dI$. Since $d \neq 0$, this implies that $i_1 + i_2 \in I$.

- Let $i \in I$ and $r \in R$. Since $dI \subseteq R$ is an ideal, $rdi \in dI$, i.e., $d(ri) \in dI$. Since $d \neq 0$, this implies that $ri \in I$.

Hence, $I \subseteq \mathbb{Q}(\zeta_m)$ is an R-submodule. □

Proposition B.4.17. If $x \in \mathbb{Q}(\zeta_m)$ is a nonzero element, then $\operatorname{N}(\langle x \rangle) = |\operatorname{N}(x)|$.

Proof. Since $\mathbb{Q}(\zeta_m)$ is a field of fractions for R, $dx \in R$ for some nonzero $d \in R$. Then $d\langle x \rangle \subseteq R$, so

$$\operatorname{N}(\langle x \rangle) = \frac{\operatorname{N}(d\langle x \rangle)}{|\operatorname{N}(d)|} = \frac{\operatorname{N}(\langle dx \rangle)}{|\operatorname{N}(d)|} = \frac{|\operatorname{N}(dx)|}{|\operatorname{N}(d)|} = \frac{|\operatorname{N}(d)\operatorname{N}(x)|}{|\operatorname{N}(d)|} = |N(x)|.$$

□

Proposition B.4.18. If $I, J \subseteq \mathbb{Q}(\zeta_m)$ are fractional ideals, then $\operatorname{N}(IJ) = \operatorname{N}(I)\operatorname{N}(J)$.

Proof. If $I = 0$, then $IJ = 0$ and $\operatorname{N}(IJ) = \operatorname{N}(I) = |R|$, so the equality becomes

$$|R| = |R| \cdot \operatorname{N}(J).$$

Since R is infinite and $\operatorname{N}(J) \leq |R|$, the equality does hold.

Now assume that $I \neq 0$ and $J \neq 0$. If $d, e \in R$ are nonzero elements such that $dI, eJ \subseteq R$, then $deIJ \subseteq R$, so

$$\operatorname{N}(IJ) = \frac{\operatorname{N}(deIJ)}{|\operatorname{N}(de)|} = \frac{\operatorname{N}(dI)\operatorname{N}(eJ)}{|\operatorname{N}(d)\operatorname{N}(e)|} = \frac{\operatorname{N}(dI)}{|\operatorname{N}(d)|} \cdot \frac{\operatorname{N}(eJ)}{|\operatorname{N}(e)|} = \operatorname{N}(I)\operatorname{N}(J).$$

□

Proposition B.4.19. If $I \subseteq \mathbb{Q}(\zeta_m)$ is a nonzero fractional ideal, then

$$(\det \sigma(I))^2 = \mathrm{N}(I)^2 \Delta_{\mathbb{Q}(\zeta_m)}.$$

Proof. Let $dI \subseteq R$, where $d \in R$. By Proposition B.4.9,

$$\mathrm{N}(I)^2 \Delta_{\mathbb{Q}(\zeta_m)} = \frac{\mathrm{N}(dI)^2}{|\,\mathrm{N}(d)|^2} \Delta_{\mathbb{Q}(\zeta_m)} = \frac{(\det \sigma(dI))^2}{|\,\mathrm{N}(d)|^2}.$$

Let $b_0, \dots, b_{n-1}$ be a $\mathbb{Z}$-basis of I. Then $db_0, \dots, db_{n-1}$ is a $\mathbb{Z}$-basis of dI, so

$$\det \sigma(dI) = |\det \sigma_i(db_j)| = |\,\mathrm{N}(d)| \cdot |\det \sigma_i(b_j)| = |\,\mathrm{N}(d)| \det \sigma(I).$$

Hence, $\mathrm{N}(I)^2 \Delta_{\mathbb{Q}(\zeta_m)} = (\det \sigma(I))^2$. $\square$

Acknowledgments

This research was supported by Fusion Technology R&D Center of SK Telecom and UNIST.

Bibliography

[ACPS09] B. Applebaum, D. Cash, C. Peikert, and A. Sahai. Fast cryptographic primitives and circularsecure encryption based on hard learning problems. In CRYPTO, 595–618. 2009.

[Bab85] L. Babai. On Lovasz lattice reduction and the nearest lattice point problem. Combinatorica, 6(1):1–13, 1986. Preliminary version in STACS 1985.

[Ban93] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In ICTS, 309–325. 2012.

[Bar12] Bar-Ilan Univ. Winter School on Lattice-Based Cryptography and Applications. 2012.

[Cam14] P. Campbell, M. Groves, and D. Shepherd. Soliloquy: A Cautionary Tale, 2014.

`http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf`

[Con09] K. Conrad. The Different Ideal.

`http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/different.pdf`

[Cra15] R. Cramer, L. Ducas, C. Peikert, O. Regev. Recovering Short Generators of Principal Ideals in Cyclotomic Rings, 2015.

`https://eprint.iacr.org/2015/313.pdf`

[Ding07] J. Ding and Richard Lindner. Identifying Ideal Lattices, 2007.

`https://eprint.iacr.org/2007/322`

[GPV08] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In STOC, pages 197–206. 2008.

[Hu15] Yupu Hu and Huiwen Jia. Cryptanalysis of GGH Map, 2015.

`https://eprint.iacr.org/2015/301.pdf`

[LPR10] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. J. ACM, 2013. To appear. Preliminary version in Eurocrypt 2010.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-LWE cryptography. In EUROCRYPT, 35–54. 2013.

[LSS14] Adeline Langlois, Damien Stehle, Ron Steinfeld. GGHLite: More Efficient Multilinear Maps from Ideal Lattices. In EUROCRYPT, 239–256. 2014.

[MP12] D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In EUROCRYPT, 700–718. 2012.

[MR04] D. Micciancio and O. Regev. Worst-case to average-case reductions based on Gaussian measures. SIAM J. Comput., 37(1):267–302, 2007. Preliminary version in FOCS 2004.

[P13] C. Peikert. Tutorials from crypt@b-it 2013 summer school at Bonn University.

`http://www.cc.gatech.edu/~cpeikert`, 2013.

[Reg05] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. J. ACM, 56(6):1–40, 2009. Preliminary version in STOC 2005.

[Sma09] N.P. Smart and F. Vercauteren. Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes, 2009.

`https://eprint.iacr.org/2009/571`