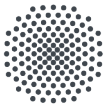

Universität Stuttgart

Masterarbeit

Sicherheit in Gitter-Basierten Kryptosystemen

Jonas Schwab

12.08.2021

Betreuer: Dr. Pascal Reisert

Institut für Informationssicherheit

Uni Stuttgart

Inhaltsverzeichnis

1 Einleitung

Die Zeit schreitet voran und mit ihr werden durch Quantencomputer viele Kryptographische Verfahren nicht mehr sicher sein. Deshalb werden in der Post-Quanten-Kryptographie Probleme betrachtet, die auch für Quantencomputer schwer zu lösen sind. Eine Sparte solcher Probleme werden durch mathematische Gitter, einer diskreten Untergruppe des euklidischen Raums $\mathbb{R}^n$, gebildet. Während in der Mathematik Gitter schon seit langer Zeit betrachtet werden, kamen erste Anwendungen in der Kryptographie mit einer einflussreichen Arbeit von Miklós Ajtai im Jahr 1996 auf. Er gab Einwegfunktionen an, die im durchschnittlichen Fall, auf der Sicherheit von Gitter-Problemen im schwersten Fall beruhen. Diese Sicherheitsaussage folgt durch eine worst-to-average-case Reduktion. Dadurch wurde das Short-Integer-Solution(SIS)-Problem erschaffen und das Interesse an Kryptographischen Verfahren, die auf Gitterproblemen basieren, wuchs. In den kommenden Jahren gab Oded Regev mit dem Learning-with-errors(LWE)-Problem ein weiteres kryptographisches Problem an, dessen Sicherheit auf Gitterproblemen im schwersten Fall beruht. Sowohl LWE als auch SIS werden in ihrer ursprünglichen Form über Matrizen aus dem Restklassenring $\mathbb{Z}_q$ definiert. Allerdings führen hohe Dimensionen, die für gewisse Sicherheitsaussagen benötigt werden, in den zugehörigen Kryptographischen Verfahren zu großen Schlüssel-Größen oder zu Problemen in der effizienten Berechnung von Multiplikationen. Um diesen Problemen Abhilfe zu schaffen werden allgemeine Ringe R, sowie darüber entstehende Module $M = R^d$ betrachtet. Dies führt zu den verallgemeinerten Problemen R-LWE,M-LWE,R-SIS und M-SIS. Zu diesen Verallgemeinerungen existieren ähnliche worst-to-average-case Reduktionen. Allerdings müssen die zugehörigen Gitter-Probleme auf bestimmte Gitter eingeschränkt werden. Die so entstehenden Mengen von Gittern werden Ideal-Gitter, beziehungsweise Modul-Gitter genannt.

In dieser Arbeit soll die Sicherheit eines Commitment-Verfahrens analysiert werden, welches von Baum et. al. in [1] definiert wurde. Während in [1] erste Reduktionsbeweise für die Hiding und Binding-Eigenschaften des Commitment-Verfahrens angegeben werden, liefert es keine detaillierten Ausführungen zur konkreten Parameterwahl und den daraus resultierenden Sicherheitsgarantien. An diesem Punkt soll diese Masterarbeit ansetzen.

Der Großteil dieser Arbeit beschäftigt sich mit einer worst-to-average-case-Reduktion der Binding-Eigenschaft des Commitment-Verfahrens. Dadurch wird die Sicherheit der Binding-Eigenschaft auf die des Modul-Short-Indepented-Vector-Problem(SIVP), im schwersten Fall, zurückgeführt. Dazu müssen verschiedene „Zwischenprobleme“ betrachtet werden. Abbildung (1) verschafft einen genauen Überblick. Wie bereits in [1] bewiesen, basiert die Sicherheit der Binding-Eigenschaft auf dem Search-Knapsack-Problem(SKS). Dieses Problem entspricht dem M-SIS-Problem in seiner Hermite-Normal-Form. Langlois und Stehlé geben in [4] eine worst-to-average case-Reduktion von Mod-SIVP zu M-SIS an, welche wir in dieser Arbeit adaptieren.

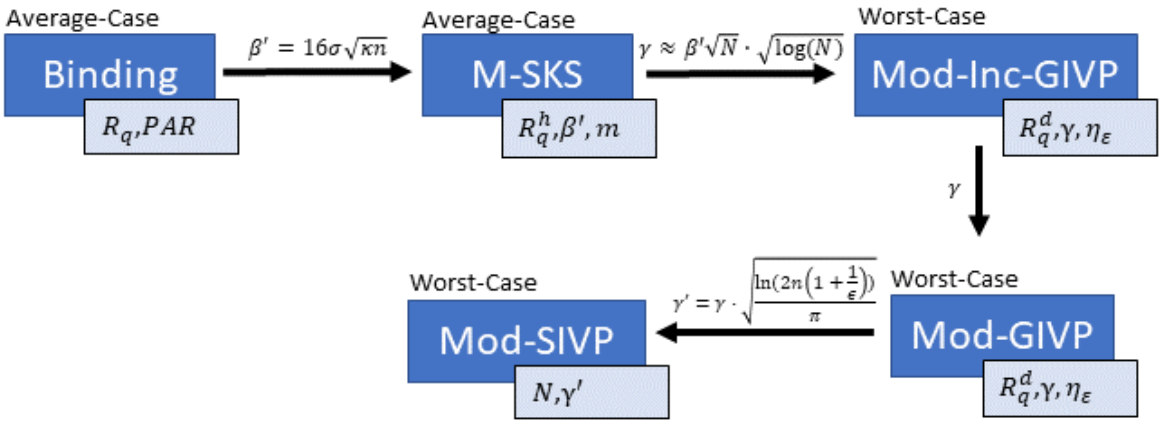

Abbildung 1: Reduktionskette - Binding - Mod-GIVP

Während in [4] die Reduktionsbeweise asymptotisch im Bezug auf die Gittergröße gehalten werden, sollen in dieser Arbeit zu bestimmten Parametern explizite Reduktionen angegeben und deren Erfolg bewiesen werden. Um diese Resultate zu erhalten, wird in Kapitel 3 ein Überblick über Gitter und die daraus resultierende diskrete Gaußverteilung geschaffen. Durch diese Erkenntnisse wird in Kapitel 5 eine detaillierte Reduktion der Binding-Eigenschaft zu gewissen Parametern angegeben. Um weitere Sicherheitsaussagen zu bekommen, werden zudem Angriffe auf die Binding und Hiding-Eigenschaft angegeben.

2 Grundlagen

In diesem Kapitel werden gängige Definitionen aus der Kryptographie und Mathematik wiederholt, die für diese Arbeit wichtig sind.

2.1 Kryptographische Grundlagen

2.1.1 Commitment-Verfahren

Ein Commitment-Verfahren besteht aus einem Tupel (gen, com) von probalistischen Turingmaschinen, welche in Polynomialzeit laufen.

- $\mathbf{gen}(1^\eta)$ gibt zu dem Sicherheitsparameter 1^η die öffentlichen Parameter des Verfahrens aus
- $\mathbf{com}(p, v)$ gibt zu gegebenem öffentlichen Parameter p und einer Nachricht v ein Commitment c aus
- $\mathbf{open}_c(p, v, r)$ überprüft ob das Commitment c zur Nachricht v gehört, bezüglich dem öffentlichen Parameter p und der Zufallsgröße r

In den meisten Commitment-Verfahren prüft der Algorithmus open ob $\text{com}^r(p, v) = c$ gilt. Wobei $\text{com}^r(p, v)$ den deterministischen Algorithmus bezeichnet, wenn com mit festgelegten Zufallsbits r ausgeführt wird. In dem in [1] beschriebenen Commitment Scheme wird der Algorithmus open etwas verändert, um ein Zero-Knowledge Protokoll mit einem validen Zero-Knowledge Proof of Knowledge anzugeben. Dazu wird ein weiter Eingabeparameter für open benötigt. Dieser ändert an den nachfolgenden Definitionen nichts. Deshalb wird in den folgenden Definitionen der Algorithmus unter den Eingabeparametern (p, v, r) betrachtet. Zu einem weiteren Parameter f kann $\text{open}_c(p, v, r)$ einfach durch $\text{open}_c(p, v, r, f)$ ersetzt werden.

Die Sicherheit eines Commitment-Verfahren hängt von den Eigenschaften Binding und Hiding ab. Binding sagt aus wie stark der Sender des Commitments an dieses gebunden ist. Hiding dagegen besagt wie schwer es für den Empfänger ist eine Information aus dem Commitment c zu erhalten. Um Sicherheitsaussagen über diese Eigenschaften zu bekommen, werden im folgenden über Security-Games Definitionen für den Vorteil eines Angreifers angegeben. Ein Security-Game zu einem bestimmen Algorithmus A ist ein probalistischer Algorithmus in Abhängigkeit von einem Sicherheitsparameter η. Die Ausgabe von $\mathbb{B}$ gibt an ob A in diesem Lauf Erfolg hatte. Dadurch ergibt sich eine Zufallsvariable, die den Erfolg eines Angreifers A misst. Wir definieren im Folgenden den Vorteil eines Angreifers A, bezüglich der Hiding- und Binding-Eigenschaft, über die zugehörigen Security-Games.

Definition 2.1 (Sicherheit-Binding) Sei $\eta \in \mathbb{N}$ und $\mathcal{C} = (\text{gen}, \text{com})$ ein Commitment-Verfahren. Sei A eine probalistische Turingmaschine. Dann wird das Security-Game $\mathbb{E}_A^{binding}$ folgendermaßen definiert:

$\mathbb{E}_{\mathbf{A}}^{\mathbf{binding}}(\eta) : \{0,1\}$

1. Generiere öffentliche Parameter:
$$p \xleftarrow{\$} \text{gen}(1^\eta)$$
2. Suche zweideutiges Commitment:
$$(v, r, v', r', c) \xleftarrow{\$} A(1^\eta, p)$$
3. Auswertung:
if $v_0 \neq v_1$ and $\text{open}_c(p, v, r) = 1 = \text{open}_c(p, v', r')$
output 1, **else output** 0

Dadurch ergibt sich der Vorteil eines Angreifers A durch:

$$Adv_A^{binding}(\eta) = \text{P}\left[\mathbb{E}_A^{binding}(1^\eta) = 1\right]$$

Definition 2.2 (Sicherheit-Hiding) Sei $\eta \in \mathbb{N}$ und $\mathcal{C} = (\text{gen}, \text{com})$ ein Commitment-Verfahren. Sei $A = (A_F, A_G)$ ein Tupel von probalistischen Turingmaschinen. Dann wird das Security-Game $\mathbb{E}_A^{hiding}$ folgendermaßen definiert:

$\mathbb{E}_{\mathbf{A}}^{\mathbf{hiding}}(\eta) : \{0,1\}$

1. Generiere öffentliche Parameter:
$$p \xleftarrow{\$} \text{gen}(1^\eta)$$
2. Finde „angreifbare“ Nachrichten:
$$v_0, v_1 \xleftarrow{\$} A_F(1^\eta, p)$$
3. Wähle zufällig eine Nachricht und ein zugehöriges Commitment:
$$b \xleftarrow{\$} \{0,1\} \ ; \ c \xleftarrow{\$} \text{com}(p, v_b)$$
4. Entscheide welche Nachricht gewählt wurde:
$$b' \xleftarrow{\$} A_G(1^\eta, p, c)$$
5. Auswertung:
if $b' = b$ **output** 1, **else output** 0

Dadurch ergibt sich der Vorteil eines Angreifers A durch:

$$Adv_A^{hiding}(\eta) = 2\left(\mathrm{P}\left[\mathbb{E}_A^{hiding}(1^\eta) = 1\right] - \frac{1}{2}\right)$$

Man sagt ein Commitment-Verfahren ist Statistical-Binding, beziehungsweise -Hiding, falls der Vorteil aller möglichen Angreifer A vernachlässigbar ist. Schränkt man die möglichen Angreifer A auf eine polyonomielle Laufzeit ein, dann spricht man von Computational-Binding, beziehungsweise -Hiding.

2.1.2 Statistische Entfernung

Die statistische Entfernung zweier Zufallsvariablen über dem selben Messraum $(\Omega, \mathcal{A})$ misst wie sehr sich diese ähneln. Da in dieser Arbeit nur diskrete Wahrscheinlichkeitsverteilungen betrachtet werden, beschränkt sich folgende Definition auf ebenjene.

Definition 2.3 Gegeben sei ein Wahrscheinlichkeitsraum (Ω, Σ, P) und ein Messraum (Ω', Σ'). Dann wird zu den Zufallsvariablen $X, Y : \Omega \to \Omega'$ die statistische Entfernung Δ folgendermaßen definiert:

$$\Delta(X, Y) = \frac{1}{2} \cdot \sum_{\omega \in \Omega'} |\mathrm{P}[X = \omega] - \mathrm{P}[Y = \omega]|.$$

Seien $X_1, \ldots, X_n$, sowie $Y_1, \ldots, Y_N$ unabhängige Zufallsvariablen. Außerdem sei f ein möglicherweise probalistischer Algorithmus. Die statistische Entfernung erfüllt unter anderem folgende Eigenschaften.

$$\Delta((X_1, \ldots, X_n), (Y_1, \ldots, Y_N)) \leq \sum_{i=1}^{n} \Delta(X_i, Y_i) \tag{2.1}$$

$$\Delta(f(X), f(Y)) \leq \Delta(X, Y) \tag{2.2}$$

Für Beweise, siehe zum Beispiel ([2],Kapitel 8.1.3).

Ein weiterer wichtiger Begriff in der Kryptographie sind die sogenannten vernachlässigbaren Funktionen. Sie fallen im asymptotischen Sinne schneller als jedes Polynom.

Definition 2.4 Eine Funktion $f : \mathbb{N} \leftarrow \mathbb{R}$ wird vernachlässigbar genannt, falls für jedes $c \in \mathbb{N}$ ein $N_c \in \mathbb{N}$ existiert, sodass für alle $n > N_c$

$$|f(n)| < \frac{1}{n^c}$$

gilt. In Landau-Notation erfüllen insbesondere Funktionen $f(n) \in n^{-\omega(1)}$ diese Eigenschaft.

2.2 Algebraische Grundlagen

Die Verallgemeinerungen des SIS- und LWE-Problems lassen sich für beliebige Ringe, beziehungsweise Module, definieren. Um jedoch die Komplexität dieser Probleme auf Gitterprobleme reduzieren zu können, benötigt man einen Zusammenhang der Ringe zu Gittern. Über Erweiterungskörper L der rationalen Zahlen $\mathbb{Q}$ können solche Ringe konstruiert werden. Der Zusammenhang ergibt sich durch Ideale, die über Einbettungen auf Gitter zurückgeführt werden können. Kreisteilungsringe liefern all diese Eigenschaften, weswegen sich Reduktionen der Modul- und Ringversionen des SIS-, sowie LWE-Problems auf Gitterprobleme ergeben. Deswegen geben wir im folgenden Kapitel einen kurzen Überblick über Kreisteilungskörper. Sie werden als Körpererweiterung von $\mathbb{Q}$ bezüglich eines Kreisteilungspolynoms Φ definiert. Das υ-te **Kreisteilungspolynom** $\Phi_\upsilon \in \mathbb{Z}[X]$ bezeichnet das ganzzahlige Minimalpolynom, mit Leitkoeffizient 1, von $p(x) = x^\upsilon - 1$. Für dieses gilt:

$$\Phi_\upsilon(X) = \prod_{j \in \mathbb{Z}_\upsilon^\times} (x - e^{2\pi i \cdot j/\upsilon}) \tag{2.3}$$

Wobei $\mathbb{Z}_\upsilon^\times$ die Einheitengruppe von $\mathbb{Z}_\upsilon$ bezeichnet. Sie ist die Menge $\mathbb{Z}_\upsilon^\times = \{z \in [\upsilon] \mid \text{ggT}(\upsilon, z) = 1\}$. Damit erhalten wir eine $\varphi(\upsilon) =: n$-dimensionale Körpererweiterung, wobei φ die eulersche φ-Funktion bezeichnet. Der Körper wird **Kreisteilungskörper** genannt und wir bezeichnen ihn fortan mit K.

$$K = \mathbb{Q}[X]/\langle \Phi_\upsilon \rangle$$

Der Kreisteilungskörper K lässt sich als Vektorraum über $\mathbb{Q}$ mit der Basis $\{1, \xi_1, \ldots, \xi_n\}$ auffassen. Hierbei bezeichnen $\xi_j = e^{2\pi i \cdot j/\upsilon}$ die Nullstellen von Φ_υ. Um nun eine Struktur zu erhalten die Gittern gleicht, betrachten wir ganzalgebraischen Zahlen bezüglich unserer Körpererweiterung $K : \mathbb{Q}$. Ein Element $z \in K$ wird ganzalgebraisch genannt, falls es eine Nullstelle eines ganzzahligen Polynoms $p(X) \in \mathbb{Z}[X]$ ist. Diese Menge wird Kreisteilungsring genannt und fortan mit R bezeichnet.

$$R := \{z \in K \mid \exists\ p(X) \in \mathbb{Z}[X] :\ p(z) = 0\}$$

Diese Menge bildet ein Integritätsbereich, dass heißt einen nullteilerfreien Ring mit $1 \neq 0$. Er wird auch Zahlbereich oder Ganzheitsring genannt. Die Elemente $\xi^j \in K$, für alle $j \in \mathbb{Z}_\upsilon^\times$, sind Nullstellen des ganzzahligen Polynoms $x^\upsilon - 1$ und somit ganzalgebraische Zahlen. Da R ein Ring ist gilt somit $\mathbb{Z}[\xi] = \sum_{j=1}^n \mathbb{Z}\xi^j \subseteq R$. Dies gilt auch für Körpererweiterungen zu beliebigen irreduziblen Polynomen $p(X)$ und deren Nullstellen $(\xi_j)_{j \in [grad(p)]}$. Für Kreisteilungskörper gilt aber insbesondere Gleichheit:

$$R = \mathbb{Z}[\xi] = \sum_{j=1}^{n} \mathbb{Z}\xi^j \subset K \tag{2.4}$$

Dies bedeutet insbesondere, dass man Elemente aus dem Kreisteilungsring R durch die $\mathbb{Z}$-Basis $(\xi_1, \ldots, xi_n)$ darstellen kann. In dieser Arbeit werden zumeist Kreisteilungspolynome Φ_{2^r} betrachtet, mit $r \in \mathbb{N}$. Es lässt sich zeigen, dass für solche Kreisteilungspolynome

$$\Phi_{2^r}(x) = x^{2^{r-1}} + 1$$

Bezeichnung	Beschreibung	Typ
Φ_υ	υ-tes Kreisteilungspolynom	$\in \mathbb{Z}[X]$
K	Kreisteilungskörper $K = \mathbb{Q}[X]/\langle\Phi_\upsilon\rangle$	Körper
R	Kreisteilungsring $\mathrm{R} = \mathbb{Z}[X]/\langle\Phi_\upsilon\rangle$	Ring
n	Dimension des Kreisteilungskörpers ($\varphi(\upsilon)$)	$\in \mathbb{N}$

Tabelle 1: Übersicht Kreisteilungskörper

gilt. Ihr zugehöriger Kreisteilungsring besitzt zudem nützliche Eigenschaften, welche im folgenden Kapitel beschrieben werden.

2.2.1 Ideale und Module

Im Folgenden soll eine kurze Übersicht wichtiger Resultate zu Idealen und Modulen in Kreisteilungsringen gegeben werden. Gebrochene Ideale eines Kreisteilungsrings R können durch eine $\mathbb{Z}$-Basis bezüglich Elementen aus dem Kreisteilungsring R aufgefasst werden. Deshalb wird ab sofort ein beliebiges Ideal $\mathcal{I}$ durch diese Basis identifiziert.

$$\mathcal{I} = \sum_{i=1}^{n} \mathbb{Z} r_i \tag{2.5}$$

Zu einer gewissen Dimension d sind Module Teilmengen von dem kartesischen Produkt K^d, die abgeschlossen unter Addition und der Multiplikation mit beliebigen Elementen aus R sind. Ab sofort wird $N = n \cdot d$ die Dimension des Moduls bezeichnet. In Kreisteilungsringen kann ein Modul M als Pseudo-Basis bezüglich den Idealen $\mathcal{I}_1, \ldots, \mathcal{I}_d \subset R$ und Elementen $b_1, \ldots, b_d \in K$ geschrieben werden:

$$M = \sum_{i=1}^{d} \mathcal{I}_i b_i \tag{2.6}$$

Der Isomorphismus θ: Für beliebige Ideale $\mathcal{I}, \mathcal{J}$ und einem gebrochenen Ideal $\mathcal{M}$ gibt Lyubashevsky in [3] einen Isomorphismus(bezüglich R-Modulen) zwischen $\mathcal{M}/\mathcal{J}\mathcal{M}$ und $\mathcal{I}\mathcal{M}/\mathcal{I}\mathcal{J}\mathcal{M}$ an. Insbesondere gibt er an, dass dieser Isomorphismus effizient berechnet und invertiert werden kann. Im Folgenden soll ein kurzer Überblick über diesen Isomorphismus geschaffen werden.

Wir beschränken uns im Folgenden auf Kreisteilungskörper. Außerdem betrachten wir das Ideal $\mathcal{J} = \langle q \rangle$, zu einer Primzahl q und $\mathcal{M} = R$. Zu einem beliebigen Ideal $\mathcal{I} \subseteq R$ und einem gewissen $t \in \mathcal{I}$ ergibt sich dann der Isomorphismus $\theta_\mathcal{I}$ zwischen R/qR und $\mathcal{I}/q\mathcal{I}$.

$$\theta_\mathcal{I} : R/qR \to \mathcal{I}/q\mathcal{I} \qquad \theta_t = t \cdot x$$

Damit θ ein Isomorphismus ist muss das durch t induzierte Ideal $t \cdot \mathcal{I}^{-1}$ teilerfremd zu $\langle q \rangle$ sein. Die Wohldefiniertheit, Surjektivität und Injektivität lassen sich direkt durch die Bedingungen nachweisen([3],Lemma 2.15). Die Existenz des Ringelements t wird durch die Primfaktorzerlegung von $\mathcal{J}$ und dem Chinesischen-Restsatz bewiesen. Insbesondere

kann t und das Inverse von θ in polynomieller Zeit berechnet werden. Adeline Langlois und Damien Stehlé fassen in [4] den Isomorphismus θ auf und verallgemeinern ihn für Module, um einen Isomorphismus zwischen $M_q = M/qM$ und $R_q^d = R^d/qR^d$ zu erhalten. Diese Verallgemeinerung wird im folgenden wiederholt. Sei M ein beliebiges Modul mit der Pseudo-Basis $(\mathcal{I}_k, b_k)_{k\in[d]}$. Dann ergibt sich der Ring-Isomorphismus

$$f : \mathcal{I}_1/q\mathcal{I}_1 \times \cdots \times \mathcal{I}_d/q\mathcal{I}_d \to M/qM \qquad f(x_1, \ldots, x_d) = \sum_{i=1}^{d} x_i \cdot b_k$$

sowie die inverse Funktion

$$f^{-1} : M/qM \to \mathcal{I}_1/q\mathcal{I}_1 \times \cdots \times \mathcal{I}_d/q\mathcal{I}_d \qquad f^{-1}(\sum_{i=1}^{d} x_i \cdot b_k) = (x_1, \ldots, x_d)$$

zwischen $\mathcal{I}_1/q\mathcal{I}_1 \times \cdots \times \mathcal{I}_d/q\mathcal{I}_d$ und M/qM. Dadurch ergibt sich durch die Isomorphismen $(\theta_{\mathcal{I}_k})_{k\in[d]}$ der Isomorphismus $\theta_M := f \circ (\theta_{\mathcal{I}_1} \times \cdots \times \theta_{\mathcal{I}_d})$:

$$\theta_M : R^d/qR^d \to M/qM \qquad \theta_M(x_1, \ldots, x_d) = f(\theta_{\mathcal{I}_1}(x_1), \ldots, \theta_{\mathcal{I}_d}(x_d)). \tag{2.7}$$

Die inverse Funktion wird dementsprechend durch $\theta_M^{-1} := (\theta_{\mathcal{I}_1}^{-1} \times \cdots \times \theta_{\mathcal{I}_d}^{-1}) \circ f^{-1}$ definiert:

$$\theta_M^{-1} : M/qM \to R^d/qR^d \qquad \theta_M^{-1}(\sum_{i=1}^{d} x_i \cdot b_k) = (\theta_{\mathcal{I}_1}^{-1} \times \cdots \times \theta_{\mathcal{I}_d}^{-1})(f^{-1}(\sum_{i=1}^{d} x_i \cdot b_k)). \tag{2.8}$$

2.2.2 Einbettungen

In diesem Kapitel werden Einbettungen definiert, um den Kreisteilungsring R als additive Teilmenge des $\mathbb{R}^n$ und somit, in den nachfolgenden Kapiteln, als Gitter auffassen zu können. Wir betrachten einen Kreisteilungskörper wie in Tabelle 1. Im folgenden werden zwei Einbettungen angegeben.

Die polynomielle Einbettung: Die polynomielle Einbettung wird fortan mit σ_{pol} bezeichnet und ergibt sich direkt über die Koeffizienten des zugehörigen Polynoms:

$$\sigma_{pol} : K \to \mathbb{R}^n \qquad z = \sum_{i=1}^{n} a_i \cdot x^i \mapsto (a_i)_{i\in[n]}$$

Die Einbettung ist ein Gruppenisomorphismus bezüglich der Addition. Da der Kreisteilungsring R die Polynome mit ganzzahligen Koeffizienten enthält, erhält man für ihn eine Einbettung nach Z^n:

$$\sigma_{pol}|_R : R \to \mathbb{Z}^n \qquad z = \sum_{i=1}^{n} a_i \cdot x^i \mapsto (a_i)_{i\in[n]}$$

Für Kreisteilungskörper mit $\upsilon = 2^r$, für ein $r \in \mathbb{N}$ lässt sich die Multiplikation von Elementen aus K folgendermaßen als Matrixmultiplikation darstellen.

$$\sigma_{pol}(y \cdot z) = \mathrm{Rot}(\sigma_{pol}(y)) \cdot \sigma_{pol}(z)$$

Wobei $\mathrm{Rot}(v)$ die Matrix bezeichnet, deren Spalten zyklische Verschiebungen von v sind:

$$\mathrm{Rot}(v) := \begin{bmatrix} v_1 & v_n & \dots & v_2 \\ v_2 & v_1 & \dots & v_3 \\ \vdots & \vdots & \ddots & \vdots \\ v_n & v_{n-1} & \dots & v_1 \end{bmatrix}$$

Insbesondere lässt sich diese Überlegung für Matrizen verallgemeinern. Sei $A \in R_q^{d \times m}$ eine Matrix über dem Ring R_q. Dann lässt sich die Multiplikation $A \cdot x$, für ein $x \in \mathbb{R}_q^m$ als Matrix-Vektor-Multiplikation über $\mathbb{Z}_q$ auffassen mit folgender Matrix:

$$\mathrm{Rot}(A) := \begin{bmatrix} \mathrm{Rot}(A_{1,1}) & \mathrm{Rot}(A_{1,2}) & \dots & \mathrm{Rot}(A_{1,m}) \\ \mathrm{Rot}(A_{2,1}) & \mathrm{Rot}(A_{2,2}) & \dots & \mathrm{Rot}(A_{2,m}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Rot}(A_{d,1}) & \mathrm{Rot}(A_{d,2}) & \dots & \mathrm{Rot}(A_{d,m}) \end{bmatrix} \in \mathbb{Z}_q^{nd \times nm} \tag{2.9}$$

Somit ergibt sich $\sigma_{pol}^{-1}(A \cdot x) = \mathrm{Rot}(A) \cdot \sigma_{pol}(x)$, wobei $\sigma_{pol}(x)$ die Komponentenweise-Abbildung von σ_{pol} auf x_i bezeichnet. Betrachtet man nun den Quotientenring R/qR, so lassen sich zu beliebigen Normen $\|\cdot\|$ über $\mathbb{R}^n$ Normen auf R/qR definieren. Für ein Polynom $p \in R_q$ mit $p = \sum_{i=1}^n a_i \cdot x^i$ werden dazu Repräsentanten$\bar{a}_i$ zu den Koeffizienten a_i aus der Menge $\{-\frac{q-1}{2}, \dots, \frac{q-1}{2}\}$ gewählt. Damit ergibt sich für $p = \sum_{i=1}^n a_i \cdot x^i$ durch die Einbettung σ_{pol} folgende Norm, die wir fortan mit $\|\cdot\|^{pol}$ bezeichnen.

$$\|p\|^{pol} := \|\sigma_{pol}(\sum_{i=1}^{n} \bar{a}_i \cdot x^i)\|$$

Dadurch ergeben sich, zusätzlich zu den Standardabschätzungen, folgende Multiplikationsabschätzungen bezüglich der euklidischen-, Summen- und Maximums-Norm:

$$\|z\|_\infty^{pol} \leq \|z\|_2^{pol} \leq \sqrt{n}\|z\|_\infty^{pol} \tag{2.10}$$

$$\|z\|_2^{pol} \leq \|z\|_1^{p} \leq \sqrt{n}\|z\|_2^{pol} \tag{2.11}$$

$$\|y \cdot z\|_\infty^{pol} \leq \|y\|_2^{p} \cdot \|z\|_2^{pol} \tag{2.12}$$

$$\|y \cdot z\|_\infty^{pol} \leq \|y\|_1^{p} \cdot \|z\|_\infty^{pol} \tag{2.13}$$

Außerdem definieren wir dazu die Menge S_β, die alle Elemente aus R_q enthält, deren Maximumsnorm maximal β beträgt

$$S_\beta := \{x \in R_q \mid \|x\|_\infty \leq \beta\}.$$

Die kanonische Einbettung: Die zweite Einbettung wird wie in ([5],Kapitel 2.1) über einen Unterraum H der Komplexen Zahlen und den kanonischen Einbettungen

$(\sigma_i)_{i\in[n]}$ definiert. Die σ_i bezeichnen dabei die n Ring-Homomorphismen von K nach $\mathbb{C}$, die Elemente aus $\mathbb{Q}$ festhalten. Durch das Auffassen von K als $\mathbb{Q}$-Vektorraum über $(1, \xi_1, \ldots, \xi_{n-1})$ lassen sie sich folgendermaßen definieren:

$$\sigma_i : K \to \mathbb{C} \qquad \sigma_i(\sum_{k=0}^{n-1} a_k \xi^k) = \sum_{k=0}^{n-1} a_k (\xi^k)^i$$

Diese werden zu einer Einbettung σ_C zusammengefasst:

$$\sigma_C : K \to \mathbb{C}^n \qquad \sigma_C = (\sigma_1, \ldots, \sigma_n)$$

Der Unterraum $H \subset \mathbb{C}^n$, der alle Elemente $h \in \mathbb{C}^n$ enthält, für die $\bar{h_i} = h_{n-i}$ gilt, lässt sich mit der Basis $h_j = \frac{1}{\sqrt{2}}(e_j + e_{\upsilon-j}), h_{\upsilon-j} = \frac{i}{\sqrt{2}}(e_j - e_{\upsilon-j})$, für $j \in [n/2]$, als reeller Vektorraum darstellen. Über diese Basis erhält man nun die Einbettung σ_H:

$$\sigma_H : K \to \mathbb{R}^n \qquad z \mapsto (a_i)_{i\in[n]} \text{ wobei } \sigma_C(z) = \sum_{i=1}^{n} a_i \cdot h_i.$$

Für eine Einbettung $\sigma = \sigma_{pol}$ oder $\sigma = \sigma_H$ definieren wir außerdem für Vektoren x aus dem Kartesischen Produkt von K^d, die Einbettung $\sigma(x)$ Komponentenweise:

$$\sigma : K^d \to \mathbb{R}^{n\times d} \qquad \sigma((x_1, \ldots, x_d)) = (\sigma(x_1), \ldots, \sigma(x_d)).$$

3 Gitter und die diskrete Normalverteilung

Die Schwierigkeit von Gitter-Problemen bilden die Grundlage für die späteren worst-to-average-case-Reduktionen. Dieser Kapitel soll einen Überblick über Gitter, die diskrete Normalverteilung sowie wichtige Aussagen darüber geben.

3.1 Gitter

Ein n-dimensionales Gitter Λ ist eine additive diskrete Untergruppe des $\mathbb{R}^n$. Sie erfüllt demnach:

- additive Untergruppe: $0 \in \mathbb{R}^n$ und für alle $u, v \in \Lambda$ gilt $u + v, -u \in \Lambda$
- diskret: Für alle $u \in \Lambda$ existiert eine Umgebung U in der x der einzige Gitterpunkt ist, also $U \cap \Lambda = \{u\}$ gilt.

3.1.1 Wichtige Begriffe

Jedes n-dimensionale Gitter besitzt eine m-dimensionale Basis von linear unabhängigen Vektoren $\mathcal{B} = \{b_1, \ldots, b_m\}$ mit $m \leq n$. Gilt Gleichheit sagen wir das Gitter besitzt *vollen Rang*. In dieser Arbeit betrachten wir immer Gittern mit vollem Rang n. Mit $\Lambda(B)$ bezeichnen wir das von der Basis B erzeuge Gitter.
Das **i-te sukzessive Minimum** des Gitters Λ wird mit $\lambda_i(\Lambda)$ bezeichnet. Es gibt das kleinst möglichste $r \in \mathbb{R}$ an, sodass es i linear unabhängige Vektoren $v_1, \ldots, v_i \in \Lambda$ gibt mit $\|v_j\| \leq r$ für alle $j = 1, \ldots, i$. Insbesondere gibt $\lambda_1(\Lambda)$ die Länge des kleinsten Vektors aus Λ an:

$$\lambda_1(\Lambda) = \min_{u \in \Lambda \setminus \{0\}} \|u\|$$

Das **Volumen** eines Gitters Λ wird über die Determinante einer beliebigen Basis B mit $\Lambda = \Lambda(B)$ definiert:

$$\mathrm{vol}(\Lambda) = \det(B) = \|\Lambda(B)\|$$

Das Volumen hängt nicht von der gewählten Basis B ab und ist damit wohldefiniert. Das zu Λ **duale Gitter** wird mit Λ^* bezeichnet und wird folgendermaßen definiert:

$$\Lambda^* := \{f \in \mathrm{Hom}(\mathbb{R}^n, \mathbb{R}) \mid \forall \lambda \in \Lambda : f(\lambda) \in \mathbb{Z}\} = \{v : \langle v, \Lambda \rangle \subset \mathbb{Z}\}$$

Das duale Gitter eines Gitters $\Lambda(B)$ erfüllt die folgenden Eigenschaften, die sich leicht nachrechnen lassen:

$$\Lambda(B)^* = \Lambda((B^T)^{-1})$$
$$\mathrm{vol}(\Lambda^*) = \mathrm{vol}(G)^{-1}$$

Zu einer Menge von Vektoren $V = (v_1, \ldots, v_n)$ bezeichnen wir mit $\tilde{V} = (\tilde{v}_1, \ldots, \tilde{v}_n)$ die zugehörigen Gram-Schmidt-Vektoren. Zu einer Basis B bilden diese im Normalfall keine Basis des Gitters, aber sind hilfreich um bestimmte Aussagen treffen zu können. Zum

Beispiel kann zu einer n-elementigen Vektormenge S, deren lineare Hülle den gesamten Raum $\mathbb{R}^n$ aufspannt und Teilmenge eines Gitters $\Lambda(B)$ ist, eine Basis B' des Gitters konstruiert werden, die „kleiner“ als S ist. Wobei „kleiner“ sich auf folgende Norm bezieht, die ab sofort für Vektormengen $V = (v_1, \ldots, v_n)$ benutzt wird:

$$\|V\| = \max_{i \in [n]} \|v_i\|_2$$

Lemma 3.1 (vgl. [2],Lemma 7.1, Seite 129) *Gegeben sei eine beliebige Basis eines n-dimensionalen Gitters $\Lambda = \Lambda(B)$ und eine Menge $S \subset \Lambda$ von Vektoren mit vollem Rang. Dann existiert ein deterministischer Algorithmus, der in polynomieller Zeit läuft und eine Basis B' von Λ zurückgibt mit*

$$\|B'\| \leq \|\tilde{S}\| \leq \|S\|$$

Von Wichtigkeit in dieser Arbeit sind unter anderem Gitter die aus Matrizen über dem Restklassenkörper $\mathbb{Z}_q$ gebildet werden. Zu einer Matrix $A \in \mathbb{Z}_q^{m \times n}$ definieren das Bild, sowie der Kern, n-dimensionale Gitter $G_q(A)$ und $G_q(A)^\perp$. Der Kern entspricht dabei dem dualen Gitter des Bildes multipliziert mit einem Skalar.

$$G_q(A) = A^T \cdot \mathbb{Z}_q^m \bmod q + q\mathbb{Z}^d \tag{3.1}$$

$$G_q(A)^\perp = \{v \in \mathbb{Z}^d \mid A \cdot v = 0 \bmod q\} \tag{3.2}$$

$$G_q(A)^* = \frac{1}{q} G_q(A)^\perp \tag{3.3}$$

3.1.2 Fundamentaler Parallelepiped

Als fundamentaler Parallelepiped wird die von einer Basis B folgendermaßen aufgespannte Fläche bezeichnet:

$$\mathcal{P}(B) = \{B \cdot x : x = (x_1, \ldots, x_n), x_i \in [0, 1[\}$$

Das Volumen einer Gitters Λ entspricht dem Flächeninhalt des von einer Basis B von Λ erzeugten Parallelepipeden $\mathcal{P}(B)$. Der Parallelepiped hängt im Gegensatz zu dem Volumen von der gewählten Basis B ab. Da ein Gitter Λ, bezüglich der Addition, eine Untergruppe von $\mathbb{R}^n$ bildet, lässt sich der Quotientenraum $\mathbb{R}^n/\Lambda$ bilden. Wobei jede Äquivalenzklasse von $\mathbb{R}^n/\Lambda$ durch ein Element von $\mathcal{P}(\Lambda)$ dargestellt werden kann.

3.1.3 Ideal- und Modul-Gitter

Durch die Einbettungen aus Kapitel 2.2.2 können Gitter zu beliebigen Modulen $M \subset K^d$ und Idealen $I \subset R$ definiert werden.[1] Wir schreiben im Folgenden σ für eine beliebige Einbettung, die ein Gruppenhomomorphismus bezüglich der Addition darstellt.[2] Durch die Darstellung von I als $\mathbb{Z}$-Basis $(r_1, \ldots, r_n)$ und der Einbettung σ erhalten wir: $\sigma(I) =$

[1] K und R, sowie die zugehörigen Parameter werden gewählt wie in Tabelle 1

[2] Inbesondere erfüllen σ_{pol} und σ_H diese Eigenschaft

$\sum_{i=1}^{n} \mathbb{Z} \cdot \sigma(r_i)$, womit $\sigma(I)$ ein Gitter zur Basis $(\sigma(r_1), \ldots, \sigma(r_n))$ darstellt. Wir schreiben Λ_I für dieses, vom Ideal I erzeugte, Gitter.

$$\Lambda_I := \sigma(I) = \sum_{i=1}^{n} \mathbb{Z} \cdot \sigma(r_i)$$

Für ein Modul $M \subset K^d$ wird analog die Pseudo-Basis $(I_k, b_k)_{k \in d}$ betrachtet, sowie die $\mathbb{Z}$-Basen $(r_1^{(k)}, \ldots, r_n^{(k)})$ der Ideale I_k. Damit erhalten wir analog

$$\sigma(M) = \sigma(\sum_{k=1}^{d} I_k b_k) = \sigma(\sum_{k=1}^{d} \sum_{i=1}^{n} (\mathbb{Z} \cdot \ r_i^{(k)}) b_k) \tag{3.4}$$

$$= \sum_{k=1}^{d} \sum_{i=1}^{n} \mathbb{Z} \cdot \sigma(r_i^{(k)} b_k). \tag{3.5}$$

Somit ist $\sigma(M)$ ein N-dimensionales Gitter bezüglich der Basis $\left(\sigma(r_i^{(k)} b_k)\right)_{i \in [n], k \in [d]}$. Wir bezeichnen die Menge der Ideal-Gitter mit Id-Λ_{R} und die Menge der Modul-Gitter bezüglich einer Dimension d mit Mod-$\Lambda_{\mathrm{R},d}$.

$$\text{Mod-}\Lambda_{\mathrm{R},d} := \{\sigma(M) \subseteq \mathbb{R}^{nd} \mid M \subseteq R^d, \text{ M ist ein Modul}\}$$

$$\text{Id-}\Lambda_{\mathrm{R}} := \{\sigma(I) \subseteq \mathbb{R}^{n} \mid I \subseteq R, \text{ I ist ein Ideal}\}$$

Die Menge der so erzeugten Gitter hängt immer von der Wahl des Kreisteilungskörper K ab.

3.2 Die diskrete Gaußverteilung

Im folgenden Abschnitt wird die diskrete Gaußverteilung definiert und es werden wichtige Sätze aus [7] wiederholt und für den Zweck dieser Arbeit reformuliert. Die Definitionen werden ähnlich gehalten wie in [8]. Wir betrachten fortan symmetrische positiv definite Kovarianzmatrizen Σ und bezeichnen Matrizen mit diesen Eigenschaften kurz mit SPD.

Definition 3.2 (Mehrdimensionale Gaußverteilung) Sei $\Sigma \in \mathbb{R}^{n \times n}$ eine SPD-Matrix. , sowie $\mu \in \mathbb{R}^n$. Die Funktion

$$\rho_\Sigma : \mathbb{R}^n \to \mathbb{R}_+ \qquad x \mapsto \frac{1}{\sqrt{\det(\Sigma)}} e^{-\pi (x-\mu)^T \Sigma^{-1} (x-\mu)}$$

ist die Dichtefunktion der mehrdimensionalen Gaußverteilung mit Erwartungswert μ und Kovarianzmatrix Σ. Oft betrachten wir Kovarianzmatrizen der Form $\Sigma = \sigma^2 \cdot \mathrm{I}_n$ für $\sigma \in \mathbb{R}$ und bezeichnen die zugehörige Dichtefunktion mit ρ_σ.

Über die Dichtefunktion und Normalisierung lässt sich auf klassischem Weg eine diskrete Verteilung über beliebige Gitter formulieren.

Definition 3.3 Sei $\Lambda \in \mathbb{R}^n$ ein Gitter. Sei Σ eine beliebige Kovarianzmatrix und $\mu \in \mathbb{R}^n$. Dann erhalten wir mit der Funktion

$$\rho_\Sigma(\Lambda' + \mu) := \sum_{\lambda \in \Lambda'} \rho_\Sigma(\lambda + \mu)$$

und Normalisierung zu einer Wahrscheinlichkeitsfunktion die diskrete Normalverteilung über $\Lambda + \mu$:

$$D_{\Lambda,\Sigma,\mu} : \Lambda + \mu \to \mathbb{R}_+ \qquad \Lambda + \mu \mapsto \frac{\rho_\Sigma(\lambda - \mu)}{\rho_\Sigma(\Lambda - \mu)}$$

Um Eigenschaften der stetigen Gaußverteilung auch auf die diskrete Verteilung übertragen zu können, wird der sogenannte Glattheitsparameter benötigt. Er gibt an wie groß die Varianz gewählt werden muss, dass zu einem bestimmten Gitter immer noch gewisse Eigenschaften gelten, die für stetige Normalverteilungen gelten. Zum Beispiel erhält man eine Aussage (3.6), dass Verschiebungen des Gitters an dem Maß $\rho_\Sigma(\Lambda)$ nicht viel ändern, wenn die Varianz mindestens so groß wie der Glattheitsparameter ist. Anschaulich streckt die Varianz das Gitter und senkt somit die diskret bedingten Sprünge des Maßes zwischen den Gitterpunkten. Um Aussagen über den Glattheitsparameter beweisen zu können, wird die Poisson-Summen Formel benötigt. Sie ist eine Konsequenz der Fouriertransformation. Für eine Funktion $f \in \mathfrak{F}$ bezeichnen wir ab sofort mit $\hat{f}$ ihre Fouriertransformation:

$$\begin{aligned} \mathcal{F} : \mathfrak{F}(\mathbb{R}^n) &\to \mathfrak{F}(\mathbb{R}^n) \\ f \to \hat{f} &:= \left\{ y \to \int_{\mathbb{R}^n} f(x) e^{-2\pi i \langle x,y \rangle} \right\}. \end{aligned}$$

Dabei bezeichnet $\mathfrak{F}$ den Raum der Funktionen, für den diese Definition Sinn macht. Die Dichtefunktion der Normalverteilung erfüllt diese Voraussetzungen und es gilt insbesondere:

$$\hat{\rho}_\Sigma = \frac{1}{\sqrt{\det(\Sigma)}} \rho_{\Sigma^{-1}} \tag{3.6}$$

Für Funktionen aus $\mathfrak{F}$ folgt nun die Poisson-Formel. Einen tieferen Einblick zur Fouriertransformation in der Kryptographie und einen Beweis für Lemma 3.4 erhält man zum Beispiel in [9].

Lemma 3.4 (Poisson-Formel) *Sei $f \in \mathfrak{F}(\mathbb{R}^n)$. Dann gilt für beliebige Gitter Λ die Poisson-Summen-Formel:*

$$f(\Lambda) = \det(\Lambda^*) \hat{f}(\Lambda^*).$$

Insbesondere gilt damit für Gitter Λ und einer SPD-Matrix Σ:

$$\rho_\Sigma(\Lambda) = \frac{\det(\Lambda^*)}{\sqrt{\det \Sigma}} \rho_{\Sigma^{-1}}(\Lambda^*) \tag{3.7}$$

Definition 3.5 Gegeben sei eine SPD-Matrix Σ und ein Gitter $\Lambda \in \mathbb{R}^n$. Dann wird Σ **ϵ-glatt** bezüglich Λ genannt falls folgende Ungleichung gilt:

$$\det(\Lambda) \cdot \rho_\Sigma(\Lambda) \leq 1 + \epsilon \tag{3.8}$$

Betrachten wir $\Sigma = \sigma^2 \mathrm{I}_n$, so bezeichnen wir mit $\eta_\epsilon(\Lambda)$ das kleinste σ, sodass Σ ϵ-glatt bezüglich Λ ist. $\eta_\epsilon(\Lambda)$ wird auch **Glattheitsparameter** genannt.
Durch die Poisson-Formel lässt sich zudem (3.8) in folgende Ungleichung umschreiben.

$$\det(\Sigma^{-1})\rho_{\Sigma^{-1}}(\Lambda^*) \leq 1 + \epsilon \tag{3.9}$$

Das folgende Lemma ist essentiell für die späteren worst-to-average case Reduktionen. Sei $\mu \in \mathbb{R}^n$ und ein Gitter Λ gegeben. Dann besagt das Lemma, dass $\rho_\Sigma(\Lambda - \mu)$ in einer kleinen Umgebung um $\det(\Lambda^*)$ liegt, falls Σ ϵ-glatt bezüglich Λ ist. Betrachtet man nun die durch $\rho_\Sigma(\Lambda - \mu)$ induzierte Verteilung $\Psi_{\Sigma,\Lambda}(\mu)$ über dem Parallelepiped $\mathbb{R}^n/\Lambda = \mathcal{P}(\Lambda)$. Dann beträgt die statistische Distanz zwischen $\Psi_{\Sigma,\Lambda}$ und der Gleichverteilung über $\mathcal{P}(\Lambda)$ gerade $\frac{1}{2}\epsilon$.

$$\begin{aligned} 2 \cdot \Delta(\Psi_{\Sigma,\Lambda}, U(\mathcal{P}(\Lambda))) &= \int_{\mathcal{P}(\Lambda)} |\Psi_{\Sigma,\Lambda}(\mu) - \frac{1}{\det(\Lambda)}| d\mu \\ &= \int_{\mathcal{P}(\Lambda)} |\rho_\Sigma(\Lambda - \mu) - \frac{1}{\det(\Lambda)}| d\mu \\ &\leq \int_{\mathcal{P}(\Lambda)} \frac{1}{\det(\Lambda)} \epsilon = \epsilon \end{aligned}$$

Dies lässt sich noch weiter ausführen. Sei $\Lambda' \subset \Lambda$ ein beliebiges Untergitter und sei V die zu der Zufallsvariable $X = Y \bmod \Lambda'$ gehörende Verteilung über Λ/Λ'. Wobei $Y \sim D_{\Lambda,\Sigma,\mu}$ die Zufallsvariable zur Normalverteilung über Λ bezeichnet. Dann ist $V([\lambda]) = \frac{\rho_\Sigma(\lambda+\Lambda')}{\rho_\Sigma(\Lambda)}$ für beliebiges $[\lambda] \in \Lambda/\Lambda'$ und die statistische Distanz zur Gleichverteilung $U(\Lambda/\Lambda')$ beträgt ϵ, falls die Kovarianzmatrix ϵ-glatt bezüglich Λ' ist, siehe Korollar 3.7. Eine weitere Folgerung von Lemma 3.6 ist Korollar 3.8. Das Korollar gibt eine obere Schranke für das diskrete Maß $\rho_\Sigma(\Lambda \cap U)$ von jedem beliebigen maximal $n-1$ dimensionalen Unterraum $\mathrm{U} \subset \mathbb{R}^n$ an.

Lemma 3.6 (vgl. [8], Lemma 3.32) *Für beliebiges $\mu \in \mathbb{R}^n$, und einer SPD-Matrix Σ, die ϵ-glatt bzgl. Λ ist gilt:*

$$\rho_\Sigma(\Lambda - \mu) \in \det(\Lambda^*) \cdot \ ]1 - \epsilon, 1 + \epsilon[\tag{3.10}$$

Korollar 3.7 (vgl. [13], Cor. 2.8) *Gegeben seien $0 < \epsilon \leq 1/2$, Gitter $\Lambda' \subset \Lambda$ und $\Sigma \in \mathbb{R}^{n \times n}$ eine SPD-Matrix. Man betrachte die Zufallsvariablen $Y \sim D_{\Lambda,\Sigma,\mu}$ und $X = Y \bmod \Lambda'$. Ist Σ ϵ-glatt bezüglich Λ', dann gilt für die statistische Entfernung von Y zur über Λ'/Λ gleichverteilten Zufallsvariablen U:*

$$\Delta(X, U) \leq 2\epsilon$$

Insbesondere gilt:

$$\max_{[\lambda] \in \Lambda/\Lambda'} (|\mathrm{P}\left[X = [\lambda]\right] - \frac{1}{|\Lambda/\Lambda'|}|) \leq \frac{4\epsilon}{|\Lambda/\Lambda'|}$$

Beweis. Sei $[\lambda] \in \Lambda/\Lambda'$. Dann lässt sich $\mathrm{P}[X = [\lambda]]$ direkt berechnen:

$$\mathrm{P}[X = [\lambda]] = \mathrm{P}[Y \bmod \Lambda' = [\lambda]] = \frac{\rho_\Sigma(\lambda + \Lambda')}{\rho_\Sigma(\Lambda)}$$

Durch voriges Lemma gilt $\rho_\Sigma(\Lambda' - \mu) \in \det(\Lambda'^*) \cdot \,]1-\epsilon, 1+\epsilon[$ für alle $\mu \in R^n$ und damit erhalten wir, da $\rho_\Sigma(\Lambda) = \sum_{[\lambda]\in\Lambda/\Lambda'} \rho_\Sigma(\lambda + \Lambda')$ gilt, folgende Ungleichung:

$$(1-\epsilon)\det(\Lambda'^*)|\Lambda/\Lambda'| \leq \rho_\Sigma(\Lambda) \leq (1+\epsilon)\det(\Lambda'^*)|\Lambda/\Lambda'| \tag{3.11}$$

Damit lässt sich direkt die statistische Distanz berechnen:

$$\begin{aligned} 2 \cdot \Delta(U, X) &= \sum_{[\lambda]\in\Lambda/\Lambda'} |\mathrm{P}[X = [\lambda]] - \frac{1}{|\Lambda/\Lambda'|}| \\ &\leq \sum_{[\lambda]\in\Lambda/\Lambda'} \frac{1+\epsilon}{(1-\epsilon)|\Lambda/\Lambda'|} - \frac{1}{|\Lambda/\Lambda'|} \\ &\leq \sum_{[\lambda]\in\Lambda/\Lambda'} \frac{4\epsilon}{|\Lambda/\Lambda'|} \\ &= 4\epsilon \end{aligned}$$

Wobei wir angenommen haben, dass $V([\lambda]) \geq \frac{1}{|\lambda/\Lambda'|}$ gilt. Dies ist möglich, da falls $V([\lambda]) \leq \frac{1}{|\lambda/\Lambda'|}$ gelten würde, wir den Summand zu $\frac{1}{|\Lambda/\Lambda'|} - \frac{1-\epsilon}{(1+\epsilon)|\Lambda/\Lambda'|}$ abschätzen können, was wiederum kleiner als $\frac{4\epsilon}{|\Lambda/\Lambda'|}$ ist, da $\epsilon < \frac{1}{2}$ gilt. ∎

Folgendes Korollar ist eine Adaption von Lemma 3.15 aus [10]. Er liefert eine Abschätzung des Maßes eines Unterraums, der maximal $n-1$-dimensional ist.

Korollar 3.8 (vgl. [10], Lemma 3.15) *Gegeben sei ein n-dimensionales Gitter Λ, $\sigma > \sqrt{c} \cdot \eta_\epsilon(\Lambda)$, für ein $c > 1$ und ein maximal $n-1$-dimensionaler Unterraum $U \subset \mathbb{R}^n$. Dann gilt*

$$D_{\Lambda,\sigma,\mu}(\Lambda \cap U) \leq \frac{1+\epsilon}{1-\epsilon}\frac{1}{\sqrt{c+1}}.$$

Beweis. Da die Varianz in alle Richtungen die selbe ist und somit die Wahrscheinlichkeit eines Gitterpunktes nur von der Entfernung zu μ abhängt, bleibt der Wert $\rho_{\Sigma,\mu}(U)$ für beliebige Rotationen und Spiegelungen der selbe. Damit können wir o.B.d.A. annehmen, dass e_1 orthogonal auf U liegt. Sei μ' die orthogonale Projektion von μ auf $\mathcal{H}$. Damit erhalten wir:

$$\rho_{\sigma,\mu}(\Lambda \cap U) \leq \rho_{\sigma,\mu'}(\Lambda \cap U)$$

Nun multiplizieren wir mit $e^{-\pi c(\frac{x_1^2}{\sigma^2})}$ um in e_1-Richtung die Varianz zu "verkleinern". Da x_1 für alle $x \in \Lambda \cap U$ 0 ist ändert dies den Wert nicht und wir erhalten:

$$\begin{aligned} \sqrt{\det(\Sigma)}\rho_{\sigma,\mu'}(\Lambda \cap U) &= \exp\left(-\pi\left(x_1^2(\frac{\sqrt{c+1}}{\sigma})^2 + \sum_{i=2}^{n} x_i^2(\frac{1}{\sigma})^2\right)\right) \\ &= \sqrt{\det(\Sigma_{c_1})}\rho_{\Sigma_{c_1},\mu'}(\Lambda \cap U) \end{aligned} \tag{3.12}$$

Wobei $\Sigma = \mathrm{I}_n\sigma^2$ und $\Sigma_{c_1} = \mathrm{diag}(1/c \cdot \sigma^2, \sigma^2, \ldots, \sigma^2)$ die in e_1-Richtung skalierte Kovarianzmatrix bezeichnet. Sei zusätzlich $\Sigma_c = \frac{1}{c} \cdot \mathrm{I}_n\sigma^2$ die in alle Richtungen skalierte Kovarianzmatrix. Dann folgt mit (3.12)

$$D_{\Lambda,s,c}(\Lambda \cap U) = \frac{\rho_{\sigma,\mu}(\Lambda \cap U)}{\rho_{\sigma,\mu}(\Lambda)} = \frac{\frac{\sqrt{\det(\Sigma_{c_1})}}{\sqrt{\det(\mathrm{I}_n\sigma^2)}}\rho_{\Sigma_{c_1},\mu}(\Lambda \cap U)}{\rho_{\sigma,\mu}(\Lambda)}$$

Nun schätzen wir durch $\rho_{\Sigma_{c_1},\mu}(\Lambda \cap U) \leq \rho_{\Sigma_{c_1},\mu}(\Lambda)$ das Maß nach oben ab, wenden die Poisson-Summen-Formel an und erhalten mit 3.7:

$$D_{\Lambda,s,c}(\Lambda \cap U) \leq \frac{\frac{\sqrt{\det(\Sigma_{c_1})}}{\sqrt{\det(\mathrm{I}_n\sigma^2)}}\rho_{\Sigma_{c_1},\mu}(\Lambda)}{\rho_{\sigma,\mu}(\Lambda)} = \frac{\rho_{\Sigma_{c_1}^{-1},\mu}(\Lambda^*)}{\rho_{1/\sigma,\mu}(\Lambda^*)} = \frac{\sqrt{\det(\Sigma_{c_1}^{-1})}\,\rho_{\Sigma_{c_1}^{-1}}(\Lambda^* - \mu)}{\sqrt{\det(\Sigma_{c_1}^{-1})}\,\rho_{1/\sigma}(\Lambda^* - \mu)}$$

Da die Varianz von Σ_c^{-1} in jedem Diagonaleintrag größer als die von $\Sigma_{c_1}^{-1}$ ist folgt durch direktes Nachrechnen $\sqrt{\det(\Sigma_{c_1}^{-1})} \cdot \rho_{\Sigma_{c_1}^{-1}} \leq \sqrt{\det(\Sigma_c^{-1})} \cdot \rho_{\Sigma_c^{-1}}$. Damit und da nach Voraussetzung Σ_c ϵ-glatt bezüglich Λ ist folgt durch erneutes Anwenden der Poisson-Summen Formel und Lemma 3.6 die gewünschte Aussage.

$$\begin{aligned} D_{\Lambda,s,c}(\Lambda \cap U) &\leq \frac{\sqrt{\det(\Sigma_c^{-1})}}{\sqrt{\det(\Sigma^{-1})}} \frac{\rho_{\Sigma_c^{-1}}(\Lambda^* - \mu)}{\rho_{1/\sigma}(\Lambda^* - \mu)} \\ &\leq \frac{1+\epsilon}{\sqrt{c}} \frac{\sigma^n}{\rho_{1/\sigma}(\Lambda^* - \mu)} \\ &\leq \frac{1+\epsilon}{1-\epsilon} \frac{1}{\sqrt{c}} \end{aligned}$$

∎

Folgendes Lemma liefert eine Abschätzung des Glattheitsparameters zum n-ten sukzessiven Minimum eines Gitters. Für den Beweis verweisen wir auf [11].

Lemma 3.9 ([11], Lemma 3.3) *Für jedes n-dimensionale Gitter Λ und $\epsilon > 0$ gilt:*

$$\eta_\epsilon(\Lambda) \leq \sqrt{\frac{\ln(2n(1+\epsilon))}{\pi}} \cdot \lambda_n(\Lambda)$$

3.2.1 Tail-Ungleichung

In diesem Kapitel wird die Tail-Ungleichung beschrieben. Die Resultate stammen von Chris Peikert ([12]). Im folgenden wird der n-dimensionale Ball B_r um den Ursprung mit Radius r betrachtet. Dann nimmt das Maß der Elemente, die außerhalb des Balls liegen, mit r exponentiell ab. Dies lässt sich für die stetige Normalverteilung durch Integralabschätzungen direkt zeigen. Für die diskrete Verteilung ist diese Herleitung komplizierter. Statt dem Ball B_r betrachtet man die Menge $U = \{u_1, \ldots, u_d\}$ von orthonormalen Vektoren und den zugehörigen „U-Zylinder“ $\mathcal{Q}_{r,\mu}^U$.

$$\mathcal{Q}_{r,\mu}^U := \{x \in \mathbb{R}^n : \|x - \mu\|_U < r\}$$

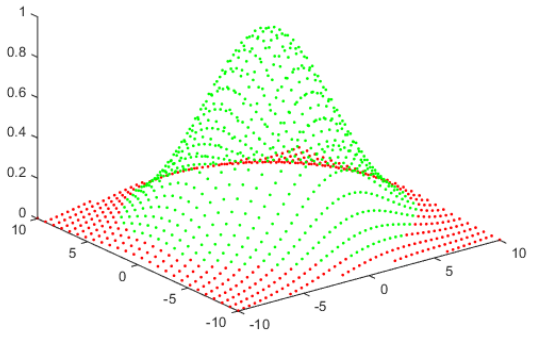

Abbildung 2: Gauß-Verteilung: Rote Punkte liegen außerhalb des Balls

Der Zylinder bezeichnet den offenen Ball um μ, mit Radius r, bezüglich der Norm $\|\cdot\|_U$. Sie gibt die Länge des Vektors (in der Summennorm) an, der durch die orthogonale Projektion auf U entsteht:

$$\|x\|_U = \sum_{i\in[d]} |\langle x, u_i\rangle|$$

Damit lässt sich nun die Tail-Ungleichung angeben. Wir verweisen auf [12] für den Beweis.

Lemma 3.10 (Tail-Ungleichung,vgl.[12],Lemma 5.1) *Gegeben sei eine Menge $U = \{u_1, \ldots, u_d\}$ von orthonormalen Vektoren. Dann gilt für jedes n-dimensionale Gitter Λ, $\mu \in \mathbb{R}^n$ und $t \geq 0$:*

$$\rho_\mu(\Lambda \setminus \mathcal{Q}^U_{t,\mu}) \leq 2^d e^{-\pi t^2/d} \cdot \rho(\Lambda)$$

Für unsere Zwecke genügt es die einelementige Menge $U = u$, für $u \in \mathbb{R}^n$ mit $\|u\|_2 = 1$, zu betrachten. Wir schreiben dementsprechend $\mathcal{Q}^u_{t,\mu}$ für den zugehörigen Zylinder und $\|\cdot\|_u$ für die zugehörige Norm. Durch die Tail-Ungleichung lässt sich nun das Maß der diskreten Gaußverteilung bezüglich der Menge $\Lambda \setminus \mathcal{Q}^u_{t,\mu}$ abschätzen. Damit erhält man folgendes Korollar:

Korollar 3.11 *Gegeben sei ein beliebiges n-dimensionale Gitter Λ, $t \geq 0, \mu \in \mathbb{R}^n$ und eine SPD Matrix Σ. Dann gilt für ein beliebiges $z \in \mathbb{R}^n$*

$$\Pr_{x\sim D_{\Lambda,\Sigma,\mu}}[|\langle \sqrt{\Sigma}^{-1}(x-\mu), z\rangle| \geq \cdot t\|z\|_2] \leq \frac{\rho_\Sigma(\Lambda)}{\rho_{\Sigma,\mu}(\Lambda)} \cdot 2e^{-\pi t^2}$$

Insbesondere gilt für $\Sigma = \sigma^2 \cdot \mathrm{I}_n$:

$$\Pr_{x\sim D_{\Lambda,\Sigma,\mu}}[|\langle x-\mu, z\rangle| \geq \cdot \sigma t\|z\|_2] \leq \frac{\rho_\Sigma(\Lambda)}{\rho_{\Sigma,\mu}(\Lambda)} \cdot 2e^{-\pi t^2}$$

Außerdem gilt insbesondere für ϵ-glatte Σ:

$$\Pr_{x\sim D_{\Lambda,\Sigma,\mu}}[|\langle \sqrt{\Sigma}^{-1}(x-\mu), z\rangle| \geq \cdot t\|z\|_2] \leq \frac{1+\epsilon}{1-\epsilon} \cdot 2e^{-\pi t^2}$$

Beweis. Wir skalieren das Gitter Λ wie in Bemerkung 3.12 und betrachten folgende Mengen:

$$\begin{aligned} M :=& \{\lambda \in \Lambda \ : \ |\langle \sqrt{\Lambda}^{-1}(\lambda - \mu), z\rangle| \geq t \cdot \|z\|_2\} \\ M' :=& \{\lambda' \in \Lambda' \ : \ |\langle (\lambda' - \mu'), z\rangle| \geq t \cdot \|z\|_2\} \end{aligned}$$

Damit gilt die Äquivalenz $\lambda \in M \Leftrightarrow \sqrt{\Lambda}^{-1}\lambda' \in M'$ und somit folgt wiederum mit Bemerkung 3.12, dass $D_{\Lambda,\Sigma,\mu}(M) = D_{\Lambda',\mathrm{I}_n,\mu'}(M')$ gilt. Da M gerade die gesuchten Ereignisse beinhaltet folgt:

$$\begin{aligned} \underset{x\sim D_{\Lambda,\Sigma,\mu}}{\mathrm{P}}[|\langle \sqrt{\Sigma}^{-1}(x-\mu), z\rangle| \geq \cdot t\|z\|_2] &= D_{\Lambda,\Sigma,\mu}(M) \\ &= D_{\Lambda',\mathrm{I}_n,\mu'}(M) \\ &= \frac{\rho_{\mu'}(M')}{\rho_{\mu'}(\Lambda')} \end{aligned}$$

Wir schreiben die Menge M' durch Division von $\|z\|_2$ und den so entstehenden normierten Vektor $u = \frac{z}{u}$ folgendermaßen um:

$$\begin{aligned} M' &= \{\lambda' \in \Lambda' \ : \ |\langle (\lambda' - \mu'), u\rangle| \geq t\} \\ &= \Lambda' \setminus \mathcal{Q}^u_{t,\mu'} \end{aligned}$$

Dadurch folgt insgesamt mit Lemma 3.10:

$$\begin{aligned} D_{\Lambda,\Sigma,\mu}(M) &= \frac{\rho(\Lambda' \setminus \mathcal{Q}^u_{t,\mu'})}{\rho_{\mu'}(\Lambda')} \\ &\leq e^{-\pi t^2} \cdot \frac{\rho(\Lambda')}{\rho_{\mu'}(\Lambda')} \\ &= e^{-\pi t^2} \cdot \frac{\rho_\Sigma(\Lambda)}{\rho_{\Sigma,\mu}(\Lambda')} \end{aligned}$$

Wobei im letzten Schritt wieder die Gleichheit der Verteilungen (Bemerkung 3.12) ausgenutzt wurde. ∎

Bemerkung 3.12 Für viele Beweise wird o.B.d.A. angenommen, dass $\Sigma = \mathrm{I}_n$ gilt. Betrachten wir die diskrete Verteilung $D_{\Lambda,\Sigma,\mu}$, zu einem beliebigen Gitter G, einer positiv definiten Matrix $\Sigma \in \mathbb{R}^{n\times n}$ und einem Erwartungsvektor $\mu \in \mathbb{R}$. Dann erhalten wir durch das skalierte Gitter $\Lambda' = \sqrt{\Sigma}^{-1}(\Lambda)$ eine zu $D_{\Lambda,\Sigma,\mu}$ identische Verteilung über Λ' mit Kovarianzmatrix I_n und Erwartungsvektor $\mu' = \sqrt{\Sigma}^{-1}\mu$. Sei $y \in \Lambda'$, dann gilt $y = \sqrt{\Sigma}^{-1}(x-\mu)$ für ein $x \in \Lambda$ und dadurch erhalten wir

$$\begin{aligned} \rho_{\Sigma,\mu}(x) &= \frac{1}{\sqrt{\Sigma}} e^{-\pi(x-\mu)^T\Sigma^{-1}(x-\mu)} \\ &= \frac{1}{\sqrt{\Sigma}} e^{-\pi(y-\sqrt{\Sigma}^{-1}\mu)^T\sqrt{\Sigma}^T\Sigma^{-1}\sqrt{\Sigma}(y-\sqrt{\Sigma}^{-1}\mu)} \\ &= \frac{1}{\sqrt{\Sigma}} \rho(y-\mu') \end{aligned}$$

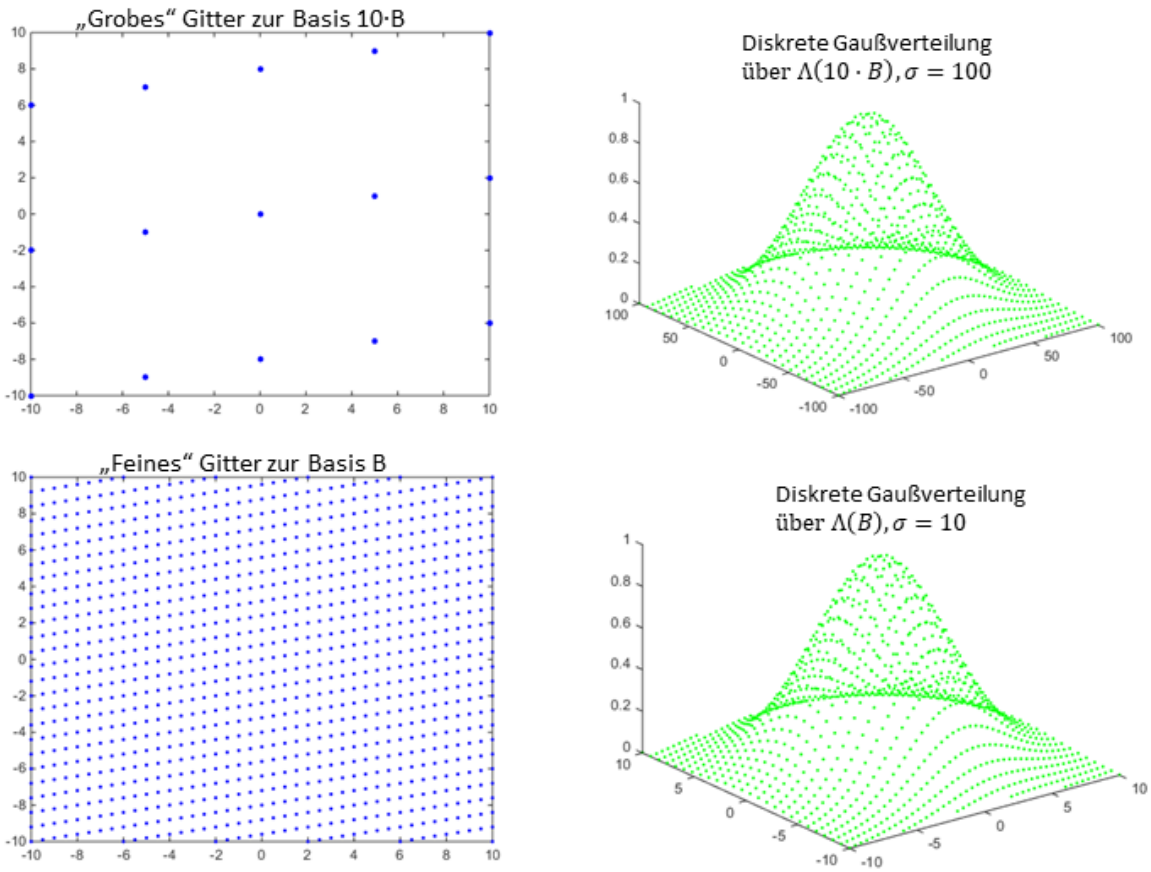

Abbildung 3: Skalierung führt zu der selben Verteilung

Damit folgt direkt, dass die Verteilungen $D_{\Lambda,\Sigma,\mu}$ und $D_{\Lambda',\mathrm{I}_n,\mu'}$ identisch sind:

$$D_{\Lambda,\Sigma,\mu}(x) = \frac{\rho_{\Sigma,\mu}(x)}{\sum\limits_{x\in\Lambda} \rho_{\Sigma,\mu}(x)} = \frac{\rho(y-\mu')}{\sum\limits_{y\in\Lambda'} \rho(y-\mu')} = D_{\Lambda',\mathrm{I}_n,\mu'}(y)$$

Ist Σ zusätzlich ϵ-glatt bezüglich Λ, so ist auch Σ' ϵ-glatt bezüglich Λ'. Dies lässt sich direkt nachrechnen. Die Abbildung 3 verdeutlicht die Überlegung.

Durch Korollar 3.11 lässt sich ein Satz zur Summe von diskreten Gaußverteilungen formulieren. Chris Peikert liefert in [12] einen Beweis für beliebige Gitter bezüglich der ∞-Norm. Wir adaptieren diese Aussage, ähnlich wie in [4] und formulieren den Satz für Module bezüglich der Einbettung σ_{pol}. In [4] wird der Satz bezüglich der Einbettung σ_H bewiesen. Er lässt sich auch direkt für beliebige Gitter Λ formulieren. Der Beweis läuft dabei immer gleich ab, indem die m Gauß-Verteilungen über M als eine Gaußverteilung über $M \times M \cdots \times M$ aufgefasst werden.

Lemma 3.13 *Sei Λ ein beliebiges Gitter und $\Sigma = UD^2U^T$ positiv definit mit einer Diagonalmatrix $D = diag(d_1, d_2, \ldots, d_n)$ und einer unitären Matrix U.*

Lemma 3.14 (vlg. [7],Lemma 4.2) *Sei Λ ein beliebiges Gitter und $\Sigma = UD^2U^T$ positiv definit mit einer Diagonalmatrix $D = diag(d_1, d_2, \ldots, d_n)$ und einer unitären Matrix U. Falls Σ zusätzlich ϵ-glatt bzgl. Λ ist gilt für ein beliebiges $z \in \mathbb{R}^n$:*

$$\underset{x \sim D_{\mathbb{Z},s,c}}{\mathrm{P}}[\langle x - c, z\rangle \geq t \cdot s] \leq 2e^{-\pi \cdot t^2} \cdot \frac{1+\epsilon}{1-\epsilon}$$

Lemma 3.15 *Sei R ein Kreisteilungsring, mit $\upsilon = 2^r$, für ein $r \in \mathbb{N}$ und $m \in \mathbb{N}$. Außerdem seien $M_i \subset R^d$, für $i \in [m]$, d-Module über K. Sei $\Sigma = \sigma^2 \mathrm{I}_N$ und $\mu_i \in R^d$ für $i \in [m]$. Ist Σ ϵ_i-glatt bezüglich $\Lambda_i = \sigma_{pol}(M_i)$ für alle $i = 1, \ldots, m$, dann gilt für alle $t > 0$ und $z \in R^m$:*

$$\underset{x_l \sim D_{\Lambda_l, \Sigma_l, \mu_l}}{\mathrm{P}}\left[\|\sum_{l=1}^{m} z_l \cdot (x_l - \mu_l)\|_\infty^{pol} \geq \sigma \cdot t\|z\|\right] \leq \prod_{l=1}^{m} \frac{1+\epsilon_l}{1-\epsilon_l} \cdot 2 \cdot N \cdot e^{-\pi t^2}.$$

Hinweis: Die Multiplikation $z_l \cdot (x_l - \mu_l)$ bezeichnet die Multiplikation im Ring R^m. Genau genommen müsste hier $z_l \cdot \sigma_{pol}^{-1}((x_l - \mu_l))$ stehen.

Beweis. Im wesentlichen wird im Beweis die Boolesche Ungleichung benutzt und durch das Zusammenfassen, der m Ziehungen aus $D_{\Lambda_l, \Sigma_l, \mu_l}$ zu einer Ziehung aus $D_{\hat{\Lambda}, \hat{\Sigma}, \hat{\mu}}$, ermöglicht Korollar 3.11 anzuwenden, wodurch wir die gewünschte Abschätzung erhalten. Wir definieren dafür

$$\begin{aligned}
\hat{\Lambda} &:= \Lambda_1 \times \Lambda_2 \times \cdots \Lambda_m \subset \mathbb{R}^{mN} \\
\hat{\Sigma} &:= \sigma^2 \cdot \mathrm{I}_{mN} \in \mathbb{R}^{mN \times mN} \\
\hat{\mu} &:= (\mu_1, \mu_2, \ldots, \mu_m) \in \mathbb{R}^{mN} \\
\hat{x} &:= (x_1, x_2, \ldots, x_m) \sim D_{\hat{\Lambda}, \hat{\Sigma}, \hat{\mu}}
\end{aligned}$$

Mit $\tilde{z}_l^i$ bezeichnen wir die i-te Zeile der Matrix $\mathrm{Rot}(z)$. Damit lässt sich wie in Kapitel 2.2.2 erwähnt für beliebiges $x \in \Lambda_i$ die Multiplikation $z_l \cdot \sigma_{pol}^{-1}(x)$ durch die Einbettung σ_{pol} folgendermaßen schreiben: $\sigma_{pol}(z_l \cdot \sigma_{pol}^{-1}(x)) = (\tilde{z}_l^i \cdot x)_{i \in [n]}$. Damit erhalten wir

$$\begin{aligned}
\sum_{l=1}^{m} \sigma_{pol}(z_l \cdot (x_l - \mu_l)) &= \sum_{l=1}^{m} \begin{bmatrix} z_l \cdot (x_l^1 - \mu_l^1) \\ \vdots \\ z_l \cdot (x_l^d - \mu_l^d) \end{bmatrix} \\
&= \begin{bmatrix} \left(\sum_{l=1}^{m} \tilde{z}_l^i (x_l^1 - \mu_l^1)\right)_{i \in [n]} \\ \vdots \\ \left(\sum_{l=1}^{m} \tilde{z}_l^i (x_l^d - \mu_l^d)\right)_{i \in [n]} \end{bmatrix}
\end{aligned} \tag{3.13}$$

, wobei $x_l^k \in \mathbb{R}^n$ den k-ten Eintrag(im Hinblick auf die Modul-Struktur) von x_i bezeichnet

und damit folgt durch 3.13 und der Booleschen Ungleichung:

$$\begin{aligned}
&\underset{x_l \sim D_{\Lambda_l,\Sigma_l,\mu_l}}{\mathrm{P}}\left[\|\sum_{l=1}^{m} z_l(x_l-\mu_l)\|_\infty^{pol} \geq t\|z\|\right] \\
&\leq \sum_{i=1}^{n}\sum_{k=1}^{d} \underset{x_l \sim D_{\Lambda_l,\Sigma_l,\mu_l}}{\mathrm{P}}\left[\underbrace{\sum_{l=1}^{m} \tilde{z}_l^i \sigma_{pol}(x_l^k-\mu_l^k)}_{:=y_{i,k}} \geq t\|z\|\right] \qquad (3.14)
\end{aligned}$$

Nun muss nur noch die hintere Summe über die Zufallsvariablen als eine Ziehung über $\hat{\Lambda}$ aufgefasst werden. Dazu betrachten wir für ein $i \in [n]$ und $k \in [d]$ die Zufallsvariable $y_{i,k}$, wie in Gleichung (3.14) definiert, und schreiben diese als eine Ziehung aus $D_{\hat{\Lambda},\hat{\Sigma},\hat{\mu}}$. Dafür definieren wir den Vektor $\hat{z_l^k} \in \mathbb{R}^{mN}$ folgendermaßen:

$$\hat{z}_{i,k} := (\underbrace{0,\ldots,0}_{N(k-1)}, \tilde{z}_1^i, \underbrace{0,\ldots,0}_{N(d-k)}, \underbrace{0,\ldots,0}_{(N)(k-1)}, \tilde{z}_2^i, \underbrace{0,\ldots,0}_{(N)(d-k)}, \underbrace{0,\ldots,0}_{N(d-k)}, \ldots, \tilde{z}_m^i, \underbrace{0,\ldots,0}_{N(d-k)}).$$

Wenn wir also mit $y(j)$ die j-te Stelle eines Vektors y bezeichnen, gilt:

$$\hat{z}_{i,k}(Nkl) = \tilde{z}_l^i(1), \hat{z}_{i,k}(Nkl+1) = \tilde{z}_l^i(1+1), \ldots \hat{z}_{i,k}(Nkl+N-1) = \tilde{z}_l^i(N).$$

Das heißt an der Nkl-ten Stelle steht gerade der Vektor $\tilde{z}_l^i$. Somit können wir $y_{i,k}$ als Skalarprodukt ausdrücken:

$$y_{i,k} = \langle \hat{z}_{i,k}, \hat{x}-\hat{\mu}\rangle$$

Da $\|\hat{z}_{i,k}\| = \|z\|$ gilt, folgt durch Normalisierung und Korollar 3.11 die gewünschte Aussage:

$$\underset{\hat{x} \sim D_{\hat{\Lambda},\hat{\Sigma},\hat{\mu}}}{\mathrm{P}}[\langle \hat{z}_{i,k}, \hat{x}-\hat{\mu}\rangle \geq t\|z\|] \leq \frac{\rho_{\hat{\Sigma}}(\hat{\Lambda})}{\rho_{\hat{\Sigma},\hat{\mu}}(\hat{\Lambda})} \cdot 2e^{-\pi t^2}$$

■

Bemerkung 3.16 Der letzte Satz wurde bezüglich der Maximumsnorm bewiesen. Durch Abschätzung der euklidischen Norm (2.10) erhalten wir direkt folgende Aussage, für Parameter gewählt wie in Lemma 3.15:

$$\underset{x_l \sim D_{\Lambda_l,\Sigma_l,\mu_l}}{\mathrm{P}}\left[\|\sum_{l=1}^{m} z_l(x_l-\mu_l)\|_2^{pol} \geq \sqrt{N}t\|z\|\right] \leq \prod_{l=1}^{m} \frac{1+\epsilon_l}{1-\epsilon_l} \cdot 2 \cdot nd \cdot e^{-\pi t^2}$$

3.2.2 Sampling-Algorithmus zur diskreten Normalverteilung

Im folgenden Kapitel wird ein probalistischer Algorithmus zum Ziehen aus einer Normalverteilung über einem beliebigem Gitter beschrieben. Er ist essentiell für die worst-to-average-case-Reduktionen des M-SIS-Problems. Der Algorithmus stammt aus einer Arbeit von Craig Gentry, Chris Peikert und Vinod Vaikuntanathan ([13]). Deren Sätze und Beweise passen wir für unsere Zwecke an.

Zuerst wird der Algorithmus SampleZ definiert, der nach der Verwerfungsmethode aus den ganzen Zahlen $\mathbb{Z}$ zieht und dessen Verteilung nahe an der diskreten Verteilung $D_{\mathbb{Z},s,c}$ liegt.

SampleZ$_\mathbf{t}$ $(s \in \mathbb{R}^+, c \in \mathbb{Z}) : \mathbb{Z}$

1. Definiere eine endliche Untermenge von $\mathbb{Z}$:
$$Z := \mathbb{Z} \cap [c - s \cdot t, c + s \cdot t]$$
2. Ziehe aus der Gleichverteilung über Z: $x \xleftarrow{\$} Z$
3. Mit Wahrscheinlichkeit $p \leftarrow \rho_s(x - c)$ output x, ansonsten springe zu 1. zurück.

Zu festen Parametern s, c, t bezeichnen wir mit SZ die Zufallsvariable, die durch die Ausgabe des Algorithmus SampleZ$_{t(n)}(s, c)$ entsteht.

Lemma 3.17 *Die Wahrscheinlichkeitsverteilung von SampleZ$_{t(n)}$ eingeschränkt auf Z ist $D_{Z,s,c}$.*

Beweis. Wir rechnen direkt nach und erhalten zu beliebigen $x \in Z$

$$P(SZ = x) = \sum_{i=0}^{\infty} P(A)^i \cdot \rho_s(x - c) \cdot \frac{1}{|Z|}, \tag{3.15}$$

wobei A das Ereignis bezeichnet, wenn der Algorithmus einen Durchlauf wiederholen muss. Es gilt $\sum_{x \in Z} P(SZ = x) = 1$ und damit folgt

$$\sum_{i=0}^{\infty} P(A)^i = \frac{|Z|}{\sum_{x \in Z} \rho_s(x - c)},$$

wodurch wir mit Einsetzen der letzten Gleichung in 3.15 die gewünschte Aussage erhalten.∎

Das Lemma 3.17 geht davon aus, dass der Algorithmus die Schleife theoretisch unendlich oft wiederholen kann. Dies ist in der Praxis natürlich nicht möglich. Deshalb kann in der Praxis eine Maximalanzahl von Durchläufen festgelegt werden. Dies führt zu einer vernachlässigbaren Abweichung zu der Verteilung $D_{Z,s,c}$, da die Wahrscheinlichkeit $P(A)^k$, dass der Algorithmus k Durchläufe hat exponentiell in k fällt.

Lemma 3.18 (vgl. [13],Lemma 4.3) *Seien $0 < \epsilon < e^{-\pi}, s \geq \eta_\epsilon(\mathbb{Z}), c \in \mathbb{R}$ gegeben. Die statistische Entfernung von $X \sim D_{\mathbb{Z},s,c}$ und der Zufallsvariable zu $SZ \sim$ SampleZ$_{t(n)}(s, c)$ beträgt:*

$$\Delta(X, SZ) \leq 2 \cdot e^{-\pi t^2} \cdot \frac{1 + \epsilon}{1 - \epsilon} \cdot \frac{\rho_{s,c}(\mathbb{Z})}{\rho_{s,c}(Z)}$$

Beweis. Da durch Lemma 3.17 die Zufallsvariable SZ nach $D_{Z,s,c}$ verteilt ist erhalten wir durch direktes nachrechnen

$$\begin{aligned}\Delta(X, SZ) &= \sum_{z\in\mathbb{Z}} |\frac{\rho_{s,c}(z)}{\rho_{s,c}(\mathbb{Z})} - \frac{\rho_{s,c}(z)}{\rho_{s,c}(Z)}| \\ &= \frac{\rho_{s,c}(\mathbb{Z})}{\rho_{s,c}(Z)} - 1\end{aligned}$$

Wir betrachten $\Delta(X, SZ) \cdot \frac{\rho_{s,c}(Z)}{\rho_{s,c}(\mathbb{Z})}$ und erhalten mit der letzten Gleichung sowie Korollar 3.11:

$$\Delta(X, SZ) \cdot \frac{\rho_{s,c}(Z)}{\rho_{s,c}(\mathbb{Z})} = \frac{\rho_{s,c}(\mathbb{Z}/Z)}{\rho_{s,c}(\mathbb{Z})} = \Pr_{x\sim D_{\mathbb{Z},s,c}}[|x-c| \geq t\cdot s] \leq 2e^{-\pi\cdot t^2}\cdot\frac{1+\epsilon}{1-\epsilon}.$$

Durch Multiplikation mit $\frac{\rho_{s,c}(\mathbb{Z})}{\rho_{s,c}(Z)}$ folgt nun die gewünschte Aussage. ∎

Durch Lemma 3.17 folgt insbesondere, dass für Parameter t, die schneller wachsen als $\log(n)$, die statistische Distanz vernachlässigbar wird.
Mit Hilfe des Algorithmus SampleZ lässt sich nun ein probalistischer Algorithmus definieren, der Gitterpunkte aus einem beliebigen Gitter Λ zieht und dessen Verteilung nahe an der diskreten Verteilung $D_{\Lambda,s,c}$ liegt. Für eine orthonormale Basis B wäre der Algorithmus einfach aufzustellen. Zu gegebenem $c = \sum_{i=1}^{n} c_i \cdot b_i$ würde er n-mal SampleZ aufrufen mit $z_i \leftarrow SampleZ(s, c_i)$ und den Vektor $\sum_{i=1}^{n} z_i b_i$ zurückgeben. Die Rückgabe wäre somit nahe an der Verteilung $D_{\Lambda(B),s,c}$. Für beliebige Basen muss zusätzlich noch die Länge und die Orthogonalität der b_i berücksichtigt werden. Dies passiert im folgenden Algorithmus durch die Wahl von c_i' und s' in jedem Schritt.

SampleG$(s \in \mathbb{R}^+, c \in \mathbb{R}^n, B \in \mathrm{GL}_{\mathbb{R}}(n)) : \mathbb{Z}$

1. sei $v_n \leftarrow 0$ und $c_n \leftarrow c$. **For** i $\leftarrow n, \ldots, 1$ **do**:
   (a) Sei $c_i' \leftarrow \langle c_i, \tilde{b_i}\rangle / \langle \tilde{b_i}, \tilde{b_i}\rangle$ und $s_i'/\|\tilde{b_i}\|$
   (b) Wähle $z_i \xleftarrow{\$} \mathrm{SampleZ}_{\log(n)}$
   (c) Sei $c_{i-1} \leftarrow c_i - z_i b_i$ und sei $v_{i-1} \leftarrow v_i + z_i b_i$
2. **Output** v_0

Für den ausführlichen Beweis verweisen wir auf ([13]),Kapitel 4.2).

Lemma 3.19 *Gegeben sei eine Basis B eines n-dimensionalen Gitters $\Lambda = \Lambda(B)$, eine gewünschte Varianz $s \geq \|\tilde{B}\|\omega(\sqrt{\log n})$ und der gewünschte Erwartungsvektor $c \in \mathbb{R}^n$. Dann ist die statistische Entfernung zwischen der Verteilung des Algorithmus SampleG und der diskreten Gaußverteilung $D_{\Lambda,s,c}$ vernachlässigbar.*

4 Probleme auf Gittern

Zu einer beliebigen Norm $\|\cdot\|$ lassen sich die folgenden Probleme definieren. Wir gehen dabei von Gittern in $\mathbb{R}^n$ aus. Die Approximations-Varianten der Gitterprobleme hängen dabei von dem sogenannten Approximationsfaktor γ ab. Er ist im allgemeinen eine Funktion

$$\gamma : \mathbb{N} \to \mathbb{R}_+$$

und gibt in Abhängigkeit von der Dimension des Gitters an, wie gut die Lösung sein muss. Wir geben im folgenden Definitionen für in dieser Arbeit relevante Gitter-Probleme an.

Definition 4.1 (Shortest Vector Problem)(SVP)
Gegeben sei eine Basis $\mathcal{B}$ eines Gitters Λ. Finde den kleinsten Vektor $v \in \Lambda \setminus \{0\}$ bzgl. $\|\cdot\|$, d.h.:

$$\|v\| = \lambda_1(\Lambda)$$

Definition 4.2 (Approximate Shortest Vector Problem)(SVP_γ)
Gegeben sei eine Basis $\mathcal{B}$ eines Gitters Λ. Finde einen Vektor $v \in \Lambda \setminus \{0\}$ der klein genug bzgl. γ und $\|\cdot\|$ ist, d.h.

$$\|v\| \leq \gamma(n) \cdot \lambda_1(\Lambda)$$

Definition 4.3 (Approximate Shortest Independent Vector Problem)(SIVP_γ)
Gegeben sei eine Basis $\mathcal{B}$ eines Gitters Λ mit vollem Rang. Finde n linear unabhängig Vektoren $v_1, \ldots, v_n \in \Lambda$ für die gilt:

$$\|v_i\| \leq \gamma(n) \cdot \lambda_n(\Lambda) \qquad \text{für alle } i = 1, \ldots, n$$

Definition 4.4 (Generalized Independent Vector Problem($\mathbf{GIVP}_\gamma^{n_\epsilon}$)) Gegeben sei eine Basis $\mathcal{B}$ eines Gitters mit vollem Rang. Finde n linear unabhängig Vektoren $v_1, \ldots, v_n \in \Lambda$ für die gilt:

$$\|v_i\| \leq \gamma(n) \cdot \eta_\epsilon(\Lambda(B)) \qquad \text{für alle } i = 1, \ldots, n$$

Definition 4.5 (Incremental Generalized Independent Vector Problem(Inc-$\mathbf{GIVP}_\gamma^{n_\epsilon}$))
Gegeben sei das Tupel $(B, S, \mathcal{H})$ mit:

- B: Basis eines n-dimensionalen Gitters
- $S \subseteq \Lambda(B)$: Menge von Gitterpunkten, mit vollem Rang n und $\|S\| \geq \gamma(n) \cdot \eta_\epsilon(\Lambda(B))$
- $\mathcal{H} \subset \mathbb{R}^n$: n-1 dimensionale Hyperebene von $\mathbb{R}^n$

Finde $h \in \Lambda(B) \setminus \mathcal{H}$, sodass $\|h\| \leq \|S\|/2$ gilt.

Betrachten wir die Probleme bezüglich eines Kreisteilungsringes R mit einer Einbettung σ, wie in 3.1.3. Dann bezeichnen wir die Einschränkung der Probleme auf Modul- beziehungsweise Ideal-Gitter mit I_R- respektive Mod_R- vor dem Namen.

4.1 Komplexität von Gitter Problemen

Die Komplexität von Gitter-Problemen hängt von dem Approximationsfaktor γ ab. Während es für exponentielle Faktoren, dass heißt $\gamma \in O(2^n)$, effiziente Algorithmen zur Lösung der Probleme SIVP_γ und SVP_γ gibt, wird für konstante Approximationsfaktoren NP-Schwere angenommen. Basis-Reduktionsverfahren liefern solche Lösungen. Sie versuchen iterativ eine gegebene Basis B in jedem Schritt zu verbessern, in dem Sinne, dass die Basisvektoren möglichst klein werden. Dies führt insbesondere dazu, dass die Vektoren nach jedem Schritt „orthogonaler “ zueinander stehen. Das bekannteste Basis-Reduktionsverfahren ist der LLL-Algorithmus. Ein weiteres Basis-Reduktionsverfahren ist der von Schnorr und Euchner beschriebene BKZ-Algorithmus. Er liefert bessere Heuristische Ergebnisse im Bezug auf die Laufzeit. Um genaue Aussagen über die Laufzeit von LLL und BKZ machen zu können, wird der Hermite-Faktor δ_0^n benutzt. Der Hermite-Faktor misst wie gut eine gewisse Basis B zu einem Gitter Λ reduziert ist.

Definition 4.6 (Hermite-Faktor $\boldsymbol{\delta_0^n}$) Sei Λ ein Gitter und $\{b_0, \ldots, b_{n-1}\}$ eine geordnete Basis, das heißt $\|b_0\| \leq \|b_1\| \cdots \leq \|b_{n-1}\|$. Der Hermite-Faktor δ_0^n wird bestimmt durch folgende Gleichung:

$$\|b_0\|_2 = \delta_0^n \cdot vol(\Lambda)^{1/n}$$

Eine Schätzung der Laufzeit, in Abhängigkeit des Hermite-Faktors δ_0, geben Lindner und Peikert in [14] an. Sie kommen auf eine logarithmische Laufzeit von

$$\log t(\delta_0) = \frac{1.8}{\log \delta_0} - 110.$$

Dies führt, in Anbetracht auf die Rechenleistung des benutzten Computers([15]), auf eine geschätzte Anzahl von

$$c = 2^{\frac{1.8}{\log \delta_0} - 78.9} \tag{4.1}$$

Taktzyklen. Eine weitere Schätzung des BKZ(2.0)-Algorithmus liefert Albrecht in [16]. Er kommt auf eine Laufzeit von

$$\log t(\delta_0) = \frac{0.009}{\log^2 \delta_0} - 27.$$

Dies führt wiederum zu

$$c = 2^{\frac{0.009}{\log^2 \delta_0} + 4.1} \tag{4.2}$$

Taktzyklen.

4.2 Das SIS-Problem

Das Short-Integer-Solution Problem wurde 1996 von großer Bedeutung als Ajtai in einer Arbeit Einwegfunktionen angab, die auf dem SIS-Problem beruhen. Er führte die Schwierigkeit des SIS-Problem im Durchschnittsfall auf die des SIVP-Problems im schwersten Fall zurück. Im Jahr 1997 beschrieb er in einer nachfolgenden Arbeit ein erstes Gitter-Basiertes öffentliches Verschlüsselungsverfahren. Darauf aufbauend wurden seitdem weitere Gitter-Basierte Kryptographische Verfahren beschrieben, die auf dem SIS-Problem beruhen. In diesem Kapitel werden das SIS Problem und Verallgemeinerungen des Problems auf Ringe(R-SIS), sowie Module(M-SIS) definiert und beschrieben. Die Binding Eigenschaft des in [1] beschriebenen Commitement-Verfahrens beruht auf dem Search Knapsack Problem(SKS). Es beschreibt das MSIS-Problem in seiner Hermitischen Normalform. Es werden im Folgenden die verschiedenen Probleme definiert für fest gewählte beliebige Parameter $q, n, m \in \mathbb{N}$ und einem Kreisteilungsring R, mit Dimension n.

Definition 4.7 (Short Integer Solution)($\mathrm{SIS}^2_{n,q,\beta,m}$)
Gegeben sei eine Matrix $A \in \mathbb{Z}_q^{n \times m}$. Finde $z \in \mathbb{Z}^m \setminus \{0\}$ mit $\|z\| \leq \beta$, so dass

$$Az = 0^n$$

gilt. Wobei 0^n den Nullvektor in $\mathbb{Z}^n$ bezeichnet.

Definition 4.8 (Ring Short Integer Solution)(**R-**$\mathrm{SIS}^p_{R_q,\beta,m}$)
Gegeben seien $a_1, \ldots, a_m \in R_q$. Finde $z = (z_1, \ldots, z_m) \in \mathbb{R}_q^m \setminus \{0\}$ mit $\|z\|_p \leq \beta$, so dass folgendes gilt:

$$\sum_{i=1}^{m} a_i z_i = 0$$

Definition 4.9 (Module Short Integer Solution)(**M-**$\mathrm{SIS}^2_{R_q^d,\beta,m}$)
Gegeben sei eine Matrix $A = [a_1|\ldots|a_m] \in \mathbb{R}_q^{d \times m}$. Finde $z \in \mathbb{R}_q^m \setminus \{0\}$ mit $\|z\| \leq \beta$, so dass folgendes gilt:

$$Az = \sum_{i=1}^{m} a_i z_i = 0^d$$

Definition 4.10 (Search Knapsack Problem)($\mathrm{SKS}^2_{R_q^d,\beta,m}$)
Gegeben sei eine Matrix $A \in R^{d \times (m-d)}$. Finde $y \in R^m$ mit $\|y_i\| \leq \beta$ für alle $i = 1, \ldots, m$, so dass folgendes gilt:

$$\begin{bmatrix} I_d & A \end{bmatrix} \cdot y = 0^n d$$

Betrachtet man Kreisteilungsringe $R = \mathbb{Z}[X]/\langle \Phi_n \rangle$ mit $n = 2^b$ für ein $b \in \mathbb{N}$. Dann sind das M-SIS und das R-SIS-Problem Spezialfälle des SIS-Problems. Wie in 2.2.2 beschrieben lässt sich die Multiplikation in R als eine Matrixmultiplikation darstellen. Damit lässt sich das RSIS-Problem als SIS-Problem eingeschränkt auf Blockweise-Zyklische Matrizen schreiben:

$$BZM := \{A \in R^{n \times nm} \mid A = [\mathrm{Rot}(a_1)|\ldots|\mathrm{Rot}(a_m)] \text{ für } a_1, \ldots, a_m \in R^n\}$$

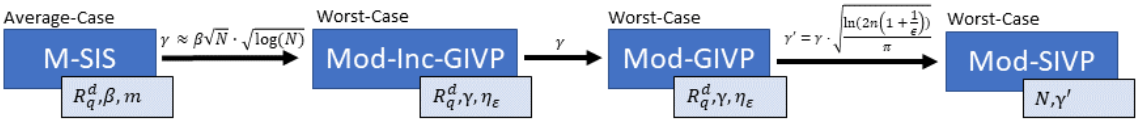

Abbildung 4: Reduktionskette

Das M-SIS-Problem lässt sich ähnlich auffassen. Hierbei betrachtet man d-fach-Blockweise-Zyklische Matrizen.

$$dBZM := \{A \in R^{nd \times nm} \mid A = \mathrm{Rot}(A'), \text{ für ein } A' \in R_q^{d \times m}\}$$

Viele Kryptographische Verfahren arbeiten mit der hermitischen Normal-Form(HNF) $\begin{bmatrix} I_d & A \end{bmatrix}$. Dies hat den Vorteil, dass weniger Speicherplatz für die Matrix A benötigt wird und Rechnungen vereinfacht werden. Diese Einschränkung um d Dimensionen führt allerdings zu keinem kryptographischen Nachteil im Bezug auf die Sicherheit. Das liegt unter anderem daran, dass die HNF zu einer Matrix A, die vollen Rang besitzt, effizient berechnet werden kann. Im nächsten Kapitel wird sowohl das MSIS-Problem als auch das SKS-Problem, unter den selben Bedingungen, auf die Sicherheit des Mod-SIVP-Problems zurückgeführt.

4.3 Worst-to-average-case Reduktion - M-SIS

Auf der Arbeit von Ajtai aufbauend, wurden die worst-to-average-case Reduktion des SIS-Problems immer genauer und es erschienen Reduktionen zu ihren Verallgemeinerungen M-SIS und R-SIS. Adeline Langlois und Damien Stehlé geben in ([4]) eine worst-to-average-case Reduktion für beliebige Kreisteilungsringe an. Wir adaptieren diese Reduktion um Sicherheitsgarantien für bestimmte Parameter zu bekommen. Die Reduktion führt die Sicherheit des M-SIS$^2_{R_q^d,\beta,m}$-Problems auf die des Mod-GIVP$^{n_\epsilon}_\gamma$-Problems zurück, indem es zuerst eine Reduktion des Inc-GIVP$^{n_\epsilon}_\gamma$-Problems zum M-SIS$^2_{R_q^d,\beta,m}$-Problem liefert und dann das Mod-GIVP$^{n_\epsilon}_\gamma$-Problem auf das Inc-GIVP$^{n_\epsilon}_\gamma$-Problem reduziert. Inc-GIVP$^{n_\epsilon}_\gamma$ dient dabei als Hilfsproblem, um die Reduktionen übersichtlicher zu halten.

Der Sicherheitsparameter $N = nd$ gibt die Dimension der Modul-Gitter an. Wie in Kapitel 3.1.3 beschrieben ergeben sich zu den Einbettungen σ_H und σ_{pol} verschiedene Räume für Modul-Gitter. Die Wahl der Einbettung ändert aber an der nachfolgenden Reduktion nichts, da nur Lemma 3.15 benötigt wird, welches für beide Einbettungen gilt. Somit wird fortan mit σ eine der beiden Einbettungen bezeichnet. Außerdem wird zu einer Basis B eines Modul-Gitters $\Lambda = \Lambda(B)$(bzgl. σ) mit M das zugehörige Modul ($M = \sigma^{-1}(\Lambda)$ bezeichnet.

4.3.1 Die Reduktion

Nachfolgend wird ein Algorithmus angegeben, der zu gewissen Parametern des M-SIS- und Mod-GIVP-Problems eine Reduktion liefert. Die Parameter werden hier beliebig gelassen und nicht eingeschränkt. In Satz 4.16 wird beschrieben wie die Parameter gewählt werden müssen damit der Algorithmus eine Polynomialzeitreduktion liefert.
Sei R ein beliebiger Kreisteilungsring und $d \geq 1$. Weiterhin seien Parameter $m, q \in \mathbb{N}, \beta, \gamma, m, \epsilon \in \mathbb{R}^+$ beliebig aber fest gewählt. Sei weiterhin $\mathcal{O}$ ein Orakel des $\text{M-SIS}^2_{R_q^d,\beta,m}$ Problems. Der Algorithmus gibt zu einer beliebigen $\text{Mod-GIVP}^{n_\epsilon}_{\gamma}$ Instanz (B, S, H) einen Lösungskandidat $h \in \Lambda(B)$ zurück.

RedMSIS$((B, S, H)) : h \in \Lambda(B)$

1. Wähle t maximal, so dass ein s existiert mit:

$$\max\left(\frac{2q}{\gamma}, \sqrt{\log N}\right) \|S\| \leq s \leq \frac{q \cdot \|S\|}{2\beta\sqrt{N} \cdot t}$$

2. Ziehe aus der diskreten Normalverteilung $D_{\Lambda(B),s,0}$ mit dem Algr. SampleG:

$$y_l \xleftarrow{\$} \text{Sample}\Lambda(s, 0, B) \qquad \text{für } l = 1, \ldots, m$$

3. Führe $y_l \in \Lambda(B)$ auf R_q^d zurück mit dem Isomorphismus θ:

$$a_l \leftarrow \theta^{-1}(\sigma^{-1}(y_l \bmod q\Lambda)) \qquad \text{für } l = 1, \ldots, m$$

4. Führe das Orakel $\mathcal{O}$ aus:

$$z_l \leftarrow \mathcal{O}(a_1, \ldots, a_m) \qquad \text{für } l = 1, \ldots, m$$

5. Berechne den Lösungsvektor h:

$$h \leftarrow \frac{1}{q} \sum_{l=1}^{m} z_l \cdot y_l$$

6. **Output** $\sigma(h)$.

Illustration der Reduktion:
Folgende Grafik eines 2-dimensionalen Gitters verdeutlicht warum der Lösungsvektor $h = \frac{1}{q} z \cdot y$ klein ist. Das Orakel, sowie die Verteilung $D_{\Lambda(B),s,0}$ sorgen dafür, dass der Vektor $y \cdot z$ klein genug ist. Durch Skalierung mit $1/q$ wird er somit nochmal deutlich kleiner.

Um zu beweisen, dass die Reduktion Erfolg hat, mit nicht-vernachlässigbarer Wahr-

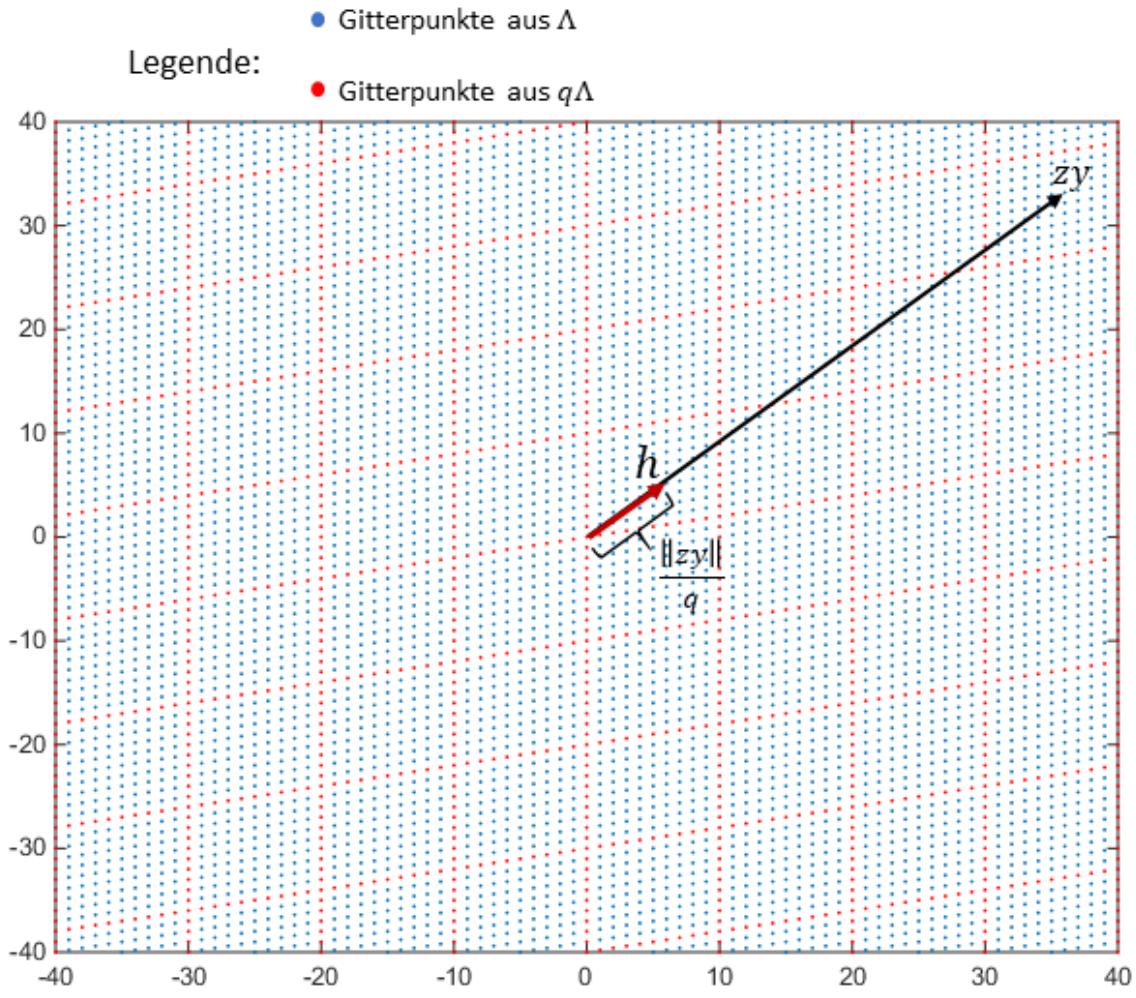

Abbildung 5: Beispielgitter zur Illustration der Reduktion

scheinlichkeit p, werden in [4] drei Aussagen bewiesen(Lemma 3.9, 3.10 und 3.11). Damit das Orakel $\mathcal{O}$ mit einer Wahrscheinlichkeit von $p = N^{-O(1)}$ erfolgreich ist muss die Verteilung von den a_l nah genug an der Gleichverteilung über R_q^d liegen. Dies wird in Lemma 3.9 bewiesen. Lemma 3.10 besagt, dass mit einer Wahrscheinlichkeit von über 1/100 der Vektor h tatsächlich nicht in der Hyperebene H liegt. Die Ungleichung $\|h\| \leq \|S\|/2$ wird, unter der Erfolgsbedingung des Orakels $\mathcal{O}$, als letztes in Lemma 3.11 nachgewiesen. Den Hilfsparameter t aus dem ersten Schritt der Reduktion führen wir ein, um zu gewissen Parametern die Erfolgswahrscheinlichkeit der Reduktion bestimmen zu können. Sie entspricht der Variable t in ([4],Lemma 3.11). Zu gewissen Parametern entspricht er damit folgendem Minimum:

$$t = \frac{1}{2\beta\sqrt{N}} \cdot \min\left(\frac{\gamma}{2}, \frac{q}{\sqrt{\log(N)}}\right). \tag{4.3}$$

Die folgenden Lemmata, die Adaptionen der drei Lemmata aus [4] sind, gehen davon aus, dass y_l nach $D_{\Lambda(B),s,0}$ verteilt ist. Da B und S den Vorgaben aus 3.1 entsprechen existiert ein Algorithmus der eine Basis T von $\Lambda(B)$ zurückgibt mit $\|\tilde{T}\| \leq \|\tilde{S}\| \leq \|S\|$. Damit folgt durch die Wahl von s, dass $s \geq \|\tilde{T}\| \cdot \sqrt{\log N}$ gilt und somit entspricht der Algorithmus SampleG aus Kapitel 3.2.2 der Verteilung $D_{\Lambda(B),s,0}$, bis auf eine vernachlässigbare statistische Distanz. Wir bezeichnen diese Distanz ab sofort mit ϵ'. In den Lemmata 4.13 und 4.14 wird von einer perfekten Ziehung aus $D_{\Lambda(B),s,0}$ ausgegangen. Um präzise zu sein nennen wir den Algorithmus, der im zweiten Schritt der Reduktion von einem $D_{\Lambda(B),s,0}$-Orakel ausgeht, RedMSIS'.

Parameter	Beschreibung	Typ
γ	Approximationsparameter für Mod-GIVP$_{\gamma}^{n_\epsilon}$	$\in \mathbb{R}_+$
β	Approximationsparameter für M-SIS$^2_{R_q^d,\beta,m}$	$\in \mathbb{R}_+$
m	Anzahl der Modulelemente des M-SIS$^2_{R_q^d,\beta,m}$ Problems	$\in \mathbb{N}$
ϵ	Genauigkeit des Glattheitsparameters	$\in \mathbb{R}_+$

Tabelle 2: Parameter zu den Problemen Mod-GIVP$_{\gamma}^{n_\epsilon}$ und M-SIS$^2_{R_q^d,\beta,m}$

Bezeichnung	Beschreibung	Typ
n	Dimension des Kreisteilungskörpers ($\phi(v)$)	$\in \mathbb{N}$
d	Dimension des Moduls R^d	$\in \mathbb{N}$
N	Dimension des entstehenden Gitters	$\in \mathbb{N}$
q	Restklassenparameter	$\in \mathbb{N}$
R	Kreisteilungsring R = $\mathbb{Z}[X]/\langle\Phi_v\rangle$	Ring

Tabelle 3: Parameter zu dem gewählten Kreisteilungsring R und dem daraus resultierenden Modul R^d

Bemerkung 4.11 Wir betrachten den Wahrscheinlichkeitsraum Ω des probalistischen Algorithmus RedMSIS. In den Lemmata 4.13 und 4.14 gehen wir davon aus, dass das Orakel Erfolg hatte. Dieses Ereignis bezeichnen wir mit OE und die bedingte Wahrscheinlichkeit dazu mit P_{OE} Dann lässt sich Ω bzw. $\Omega \cap OE$ in die Ereignisse $y' \in (M/qM)^m$ partitionieren. Sie beinhalten die Ergebnisse, in denen RedMSIS $y_l = y'_l + r_l$ annimmt für ein beliebiges $r_l \in qM$. Durch den Isomorphismus θ ist dies äquivalent dazu, dass $\theta(y'_l) = a_l$ gilt. Als nächstes betrachten wir die Zufallsvariable r_l, die den Anteil aus qM von y_l annimmt. Da das Orakel nur den y'-Anteil übergeben bekommt sind die r_l statistisch unabhängig zu den Zufallsvariablen z_l. Insbesondere ist r_l nur von y'_l abhängig. Damit folgt für fixiertes $y' = (y'_1, \ldots, y'_m)$:

$$\mathrm{P}_{OE}\left[r_l \mid (y'_1, \ldots, y'_n), (z_1, \ldots, z_n)\right] = \mathrm{P}_{OE}\left[r_l \mid (y'_1, \ldots, y'_n)\right] = \mathrm{P}_{OE}\left[r_l \mid y'_l\right]$$

Durch die Verteilung von y_l folgt also, dass die Zufallsvariable r_l für fixiertes y'_l wie die um $-y'_l$ verschobene Gaußverteilung $D_{qM,s,-y'_l}$ verteilt ist.

Lemma 4.12 ([4], vgl. Lemma 3.9) *Gegeben seien eine Instanz $(B, S, \mathcal{H})$ des* Inc-GIVP$^{n_\epsilon}_{\gamma}$*-Problems und beliebige Parameter wie in den Tabellen 3 und 2. Dann gilt für alle $l \in [m]$:*

$$\Delta((a_1, \ldots, a_m), U) \leq 2m(\epsilon + \epsilon')$$

Wobei $(a_1, \ldots, a_m)$ die Zufallsvariable aus RedMSIS bezeichnet und U die gleichverteilte Zufallsvariable aus $\mathrm{U}(M/qM)$*.*

Beweis. Die Aussage folgt direkt durch Korollar 3.7, sowie dem Isomorphismus θ und der Einbettung σ. Dies erkennt man anhand folgender Umformung der statistischen Entfernung:

$$\begin{aligned}
\Delta(a_l, U) &= \sum_{v' \in R_q^d} |\mathrm{P}[a_l = v'] - U(v')| \\
&= \sum_{v \in M_q} |\mathrm{P}[a_l = \theta^{-1}(v)] - U(v)| \\
&= \sum_{\lambda \in \Lambda_q} |\mathrm{P}[a_l = \theta^{-1}(\sigma^{-1}(\lambda))] - U(\lambda)|
\end{aligned}$$

Durch die Verteilung von $a_l = \theta^{-1}(\sigma^{-1}(y_l \bmod q\Lambda))$ folgt somit:

$$\Delta(a_l, U) = \sum_{\lambda \in \Lambda_q} |\mathrm{P}[y_l \bmod q\Lambda = \lambda] - U(\lambda)| \tag{4.4}$$

Sei nun $y'_l \sim D_{\Lambda,s,0}$. Durch die Bedingung des Lemmas gilt $\Delta(y_l, y'_l) \leq \epsilon'$. Damit erhalten wir für die statistische Distanz zwischen den Zufallsvariablen $y_l \bmod q\Lambda$ und $y'_l \bmod q\Lambda$,

durch direktes Umformen und der Dreiecksungleichung:

$$\begin{aligned}
2\Delta(y_l \bmod q\Lambda, y_l') &= \sum_{\lambda\in\Lambda_q} |\mathrm{P}[y_l \bmod q\Lambda = \lambda] - \mathrm{P}[y_l' \bmod q\Lambda = \lambda]| \\
&= \sum_{\lambda\in\Lambda_q} |\mathrm{P}[y_l = \lambda + qM] - \mathrm{P}[y_l' = \lambda + q\Lambda]| \\
&= \sum_{\lambda\in\Lambda_q} |\sum_{\lambda'\in\lambda+q\Lambda} (\mathrm{P}[y_l = \lambda'] - \mathrm{P}[y_l' = \lambda'])| \\
&= \sum_{\lambda\in\Lambda} |\mathrm{P}[y_l = \lambda] - \mathrm{P}[y_l' = \lambda]| \leq 2\epsilon' \qquad (4.5)
\end{aligned}$$

Durch die Wahl von s gilt $s \geq \frac{\sqrt{2}q}{\gamma}\|S\|$. Damit können wir Korollar 3.7 bezüglich der Verteilung y_l' mod $q\Lambda$ und den Gittern $q\Lambda$, Λ anwenden und erhalten zusammen mit (4.4), (4.5) sowie der Dreiecksungleichung folgende Aussage.

$$\Delta(a_l, U) = \sum_{\lambda\in\Lambda_q} |\mathrm{P}[y_l \bmod q\Lambda = \lambda] - U(\lambda)| \leq 2\epsilon + 2\epsilon'$$

Da die a_l unabhängig voneinander verteilt sind folgt die gewünschte Aussage. ∎

Für Lemma 4.13 und 4.14 nehmen wir an, dass $y_l \sim$

Lemma 4.13 ([4], vgl. Lemma 3.10) *Gegeben seien eine Instanz $(B, S, \mathcal{H})$ des* Inc-GIVP$^{n_\epsilon}_{\gamma}$*-Problems und beliebige Parameter wie in den Tabellen 3 und 2. Dann gilt*

$$\mathrm{P}_{OE}[\sigma(h) \notin \mathcal{H}] \geq \frac{1}{10},$$

für die Zufallsvariable h, die durch den probalistischen Algorithmus RedMSIS' entsteht.

Beweis. Ab sofort bezeichnen wir mit $\hat{\mathcal{H}}$ den zugehörigen Unterraum von $\mathcal{H}$, als Teilmenge des Moduls $M = \sigma^{-1}(\Lambda)$:

$$\hat{\mathcal{H}} = \sigma^{-1}(\mathcal{H} \cap \Lambda)$$

Wie in Bemerkung 4.11 definieren wir $y_l' = y_l \pmod{q\Lambda}$ und $r_l = y_l - y_l'$. Da das Orakel Erfolg hatte gilt $z \neq 0$. Damit existiert ein $l \in [m]$ mit $z_l \neq 0$. Ohne Beschränkung der Allgemeinheit nehmen wir $l = 1$ an. Da $\mathcal{H}$ eine Hyperebene und damit ein Unterraum von $\mathbb{R}^n$ ist liegt $\sigma(h)$ genau dann in $\mathcal{H}$ falls qh in $\mathcal{H}$ liegt. Somit folgt durch Umformung und der Gleichung $y_1 = r_1 + y_1'$, dass die Aussage $h \in \hat{\mathcal{H}}$ äquivalent zu folgender Aussage ist:

$$(r_1 + y_1') \cdot z_1 \in \mathcal{H} - \sum_{i=2}^{m} z_l \cdot y_l$$

Als nächstes multiplizieren wir mit dem Inversen von z_1 und erhalten, dass

$$r_1 \in -y_1' + \frac{1}{z_1}(\mathcal{H} - \sum_{i=2}^{m} z_l y_l) =: \mathcal{H}'$$

äquivalent zu der Aussage $h \in \hat{\mathcal{H}}$. Da $\mathcal{H}$ (N-1)-dimensional ist, kann $\hat{\mathcal{H}}$ maximal (N-1)-dimensional sein. Damit ist auch der verschobene und mit z_1 multiplizierte Raum $\mathcal{H}'$ maximal (N-1)-dimensional und es kann Korollar 3.8 verwendet werden. Wir fixieren wieder y' wie in Bemerkung 4.11. Es gilt außerdem $s \geq \sqrt{2}q\eta_\epsilon(M) = \sqrt{2}\eta_\epsilon(qM)$ und damit folgt mit Korollar 3.8

$$\begin{aligned} \mathrm{P}_{OE}\left[h \notin \mathcal{H} \mid y', z'\right] &= \mathrm{P}_{OE}\left[r_l \notin \mathcal{H}' \mid y'\right] \\ &= \underset{r_l \sim D_{qM,s,-y'_l}}{\mathrm{P}_{OE}}\left[r_l \notin \mathcal{H}'\right] \geq \frac{1}{10}. \end{aligned}$$

Anschaulich wurde hier zu festem y' und z' die Hyperebene $\mathcal{H}'$ gebildet und durch die Verteilung von r_l ergibt sich mit Hilfe von Korollar 3.8 die gewünschte Abschätzung. Der Erfolg des Orakels wird nur benötigt um ein z_l zu bestimmen mit $z_l \neq 0$. ∎

Lemma 4.14 ([4], Lemma 3.11) *Gegeben sei eine beliebige Instanz $(B, S, \mathcal{H})$ des* Inc-GIVP$^{n_\epsilon}_\gamma$ *Problems und beliebige Parameter wie in den Tabellen 3, 2. Außerdem sind $y_1, \ldots, y_m$ sowie $a_1, \ldots, a_m$ gezogen wie in RedMSIS'. Dann gilt $h \in M$ und $\|h\| \leq \|S\|/2$, unter der Bedingung dass das Orakel $\mathcal{O}$ Erfolg hat, mit einer Wahrscheinlichkeit von:*

$$\mathrm{P}_{OE}\left[\|h\| \leq \|S\|/2\right] \geq 1 - \left(\frac{1+\epsilon}{1-\epsilon}\right)^m 2 \cdot N \cdot e^{-\pi t^2}$$

Beweis. Im folgenden gilt $Az_l = 0$ und $\|z\|_2 \leq \beta$, da das Orakel Erfolg hatte. Daraus folgt direkt:

$$q \cdot h \bmod qM = \sum_{l=1}^{m} z_l \cdot y_l \bmod qM = \sum_{l=1}^{m} z_l \cdot \theta(a_l) = \theta(\sum_{l=1}^{m} z_l a_l) = 0$$

Damit liegt qh in qM und deswegen muss der Lösungsvektor h im Modul M liegen.
Als nächstes betrachten wir die Zufallsvariable $r_l = y_l - y'_l$ wie in Bemerkung 4.11. Dann folgt mit Lemma 3.15:

$$\underset{r_l \sim D_{qM,s,-y'_l}}{\mathrm{P}}\left[\|\sum_{l=1}^{m} z_l(r_l + y'_l)\|_2 \geq st\sqrt{N}\|z\|_2\right] \leq \left(\frac{1+\epsilon}{1-\epsilon}\right)^m 2 \cdot N \cdot e^{-\pi t^2}$$

Damit folgt für beliebige y' mit einer Wahrscheinlichkeit von mindestens $\left(\frac{1+\epsilon}{1-\epsilon}\right)^m 2 \cdot N \cdot e^{-\pi t^2 \cdot N}$ die benötigte Abschätzung für h

$$\|h\| = \frac{1}{q}\|\sum_{l=1}^{m} z_l \cdot y_l\| \leq \frac{st\beta\sqrt{N}}{q} \leq \frac{\|S\|}{2},$$

wobei die letzte Abschätzung aus der Ungleichung für s aus dem ersten Schritt der Reduktion folgt. ∎

Die Aussage gilt damit für beliebige Parameter. Jedoch kann das durch RedMSIS konstruierte t klein und damit auch die Wahrscheinlichkeitsabschätzung dementsprechend schlecht werden. Für genügend kleine t wird die Abschätzung negativ und damit aussagelos.

Satz 4.15 *Seien die Parameter gewählt wie in den Tabellen* 2 *und* 3. *Sei* $\mathcal{O}$ *ein Orakel, welches das* M-SIS$^2_{R_q^d,\beta,m}$ *Problem mit einer Wahrscheinlichkeit von* p *löst. Außerdem sei* ϵ' *die statistische Entfernung zwischen* SampleG$(s, 0, B)$ *und* $D_{\Lambda(B),s,0}$. *Dann löst RedMSIS das* Mod-Inc-GIVP$^{n_\epsilon}_\gamma$*-Problem mit einer Wahrscheinlichkeit* $\tilde{p}$ *von mindestens*

$$\tilde{p} \geq (p - 2m(\epsilon + \epsilon')) \left(\frac{1}{10} - \left(\frac{1+\epsilon}{1-\epsilon} \right)^m 2 \cdot N \cdot e^{-\pi t^2} - \epsilon' \right).$$

Beweis. Der Beweis ergibt sich aus Standard-Wahrscheinlichkeitsabschätzungen und der Lemmata 4.12-4.14. Gegeben sei eine Instanz $(B, S, \mathcal{H})$ des Mod-Inc-GIVP$^{n_\epsilon}_\gamma$-Problems. Wir betrachten die entstehenden Zufallsvariablen $(y_1, \ldots, y_m), (a_1, \ldots, a_m), h$. Als erstes bestimmen wir die Wahrscheinlichkeit, dass das Orakel Erfolg hat, mit Hilfe von Lemma 4.12. Dazu definieren wir $p_\mathcal{O}(A)$ als die Wahrscheinlichkeit, dass $\mathcal{O}$ zu einer bestimmten Eingabe $A \in R_q^{d \times m}$ Erfolg hat. Damit ist

$$p = \sum_{A \in R_q^{d \times m}} \frac{1}{|R_q^{d \times m}|} \cdot p_\mathcal{O}(A)$$

die gegebene Wahrscheinlichkeit, dass das Orakel zu einer gleichverteilten Eingabe Erfolg hat. Dementsprechend ist

$$p' = \sum_{A \in R_q^{d \times m}} \mathrm{P}\left[(a_1, \ldots, a_l) = A\right] \cdot p_\mathcal{O}(A)$$

die Wahrscheinlichkeit, dass das Orakel zu der nach $(a_1, \ldots, a_l)$ verteilten Zufallsvariable Erfolg hat. Dadurch ergibt sich mit Lemma 4.12, der Dreiecksungleichung und $p_\mathcal{O}(A) \leq 1$:

$$\begin{aligned} |p - p'| &= \left| \sum_{A \in R_q^{d \times m}} \left(\frac{1}{|R_q^{d \times m}|} - \mathrm{P}\left[(a_1, \ldots, a_l) = A\right] \right) \cdot p_\mathcal{O}(A) \right| \\ &\leq \sum_{A \in R_q^{d \times m}} \left| \frac{1}{|R_q^{d \times m}|} - \mathrm{P}\left[(a_1, \ldots, a_l) = A\right] \right| \leq 2m(\epsilon + \epsilon') \end{aligned}$$

Somit gilt $p' \geq p - 2m(\epsilon + \epsilon')$. Als nächstes erhalten wir durch Lemma 4.13 und 4.14 die Wahrscheinlichkeitsabschätzungen

$$\begin{aligned} \mathrm{P}_{OE}\left[\|\sigma(h')\|_2 \leq \frac{\|S\|}{2} \right] &\geq 1 - \left(\frac{1+\epsilon}{1-\epsilon} \right)^m 2 \cdot N \cdot e^{-\pi t^2} \\ \mathrm{P}_{OE}\left[\sigma(h') \notin \mathcal{H}\right] &\geq \frac{1}{10}, \end{aligned}$$

für die Zufallsvariable h' die nach RedMSIS' verteilt ist. Somit folgt durch das Additionstheorem die Abschätzung

$$\mathrm{P}_{OE}\left[\|\sigma(h')\|_2 \leq \frac{\|S\|}{2} \bigcap \sigma(h') \notin \mathcal{H} \right] \geq \frac{1}{10} - \left(\frac{1+\epsilon}{1-\epsilon} \right)^m 2 \cdot N \cdot e^{-\pi t^2}.$$

Da die statistischen Entfernung zwischen den Zufallsvariablen $y \sim \text{SampleG}$ und $y' \sim D_{\Lambda,s,0}$ nach Vorraussetzung ϵ' beträgt und die Zufallsvariablen $y_1, \ldots, y_m$ offensichtlich statistisch unabhängig sind, folgt durch die Eigenschaften (2.1) und (2.2) für statistische Distanzen die Ungleichung

$$\mathrm{P}_{OE}\left[\|\sigma(h')\|_2 \leq \frac{\|S\|}{2} \bigcap \sigma(h') \notin \mathcal{H}\right] \geq \frac{1}{10} - \left(\frac{1+\epsilon}{1-\epsilon}\right)^m 2 \cdot N \cdot e^{-\pi t^2} - \epsilon'$$

und damit die Aussage des Satzes. ∎

Nun kann ein Satz formuliert werden, der besagt wie Parameter in Abhängigkeit des Sicherheitsparameters N gewählt werden müssen, damit die Reduktion mit nicht-vernachlässigbarem Vorteil erfolgreich ist. Dabei wird die Konstante c betrachtet. Diese spielt in der asymptotischen Betrachtung des Approximationsfaktors keine Rolle. Sie ändert aber die Größe des benötigten Restklassenparameters q. Dies kann in der Praxis zu einem kleineren Nachrichtenraum führen.

Satz 4.16 *Sei $c > 1$. Für alle $d \geq 1$ und $\epsilon(N) = N^{-\sqrt{\log(N)}}$ existiert eine probalistische Reduktion von* Mod-GIVP$^{n_\epsilon}_{\gamma}$ *zu* M-SIS$^2_{R^d_q,\beta,m}$ *mit einer nicht vernachlässigbaren Wahrscheinlichkeit für alle Parameter, die wie in den Tabellen 2 und 3 gewählt sind und folgende Ungleichungen erfüllen:*

$$\gamma(N) \geq 4 \cdot \sqrt{\frac{c}{\pi}} \cdot \beta\sqrt{N} \cdot \sqrt{\log(N)} \tag{4.6}$$

$$q(N) \geq 2 \cdot \sqrt{\frac{c}{\pi}} \cdot \beta \cdot \sqrt{N} \cdot \log(N) \tag{4.7}$$

$$m, log(q) \leq poly(N) \tag{4.8}$$

Insbesondere besitzt die Reduktion eine polynomielle Laufzeit, falls das Orakel in polynomieller Zeit läuft.

Beweis. Wie am Anfang des Kapitels erwähnt folgt mit Lemma 3.7, dass die statistische Distanz ϵ' zwischen 3.2.2 und der Verteilung $D_{\Lambda(B),s,0}$ vernachlässigbar ist. Durch die Wahl der Parameter folgt für den Hilfsparameter t:

$$t = \frac{1}{2\beta\sqrt{N}} \cdot \min\left(\frac{\gamma}{2}, \frac{q}{\sqrt{\log(N)}}\right) \geq \sqrt{\frac{c}{\pi} \cdot \log N}. \tag{4.9}$$

Somit ist die Reduktion durch Satz 4.15 mit einer Wahrscheinlichkeit $\tilde{p}$ von mindestens

$$\tilde{p} \geq (p - 2m(\epsilon + \epsilon'))\left(\frac{1}{10} - \left(\frac{1+\epsilon}{1-\epsilon}\right)^m 2 \cdot N \cdot N^{-c} - \epsilon'\right)$$

erfolgreich. Da nach Voraussetzung m polynomiell beschränkt und ϵ vernachlässigbar ist, liegt $\left(\frac{1+\epsilon}{1-\epsilon}\right)^m$ beliebige nahe an eins(plus einer vernachlässigbaren Funktion), für ein genügend großes N. Da außerdem $c > 1$ ist wird $N \cdot N^{-c}$ beliebig klein und somit erhalten wir insgesamt eine nicht vernachlässigbare Wahrscheinlichkeit $\tilde{p}$. Der Isomorphismus θ, die Einbettung σ, der Sample-Algorithmus SampleG und das Orakel besitzen eine polynomielle Laufzeit. Da diese jeweils m mal aufgerufen werden und m polynomiell beschränkt ist, besitzt die Reduktion eine polynomielle Laufzeit. ∎

Die letzten zwei Schritte der Reduktionskette(Abb. 4) werden allgemein bewiesen, ohne eine Einschränkung auf Modul-Gitter zu fordern. Sie sind jeweils Worst-Case zu Worst-Case Reduktionen. Damit folgt die Reduktion für jedes beliebige Gitter und somit für beliebige Einschränkungen. Der folgende Satz stammt aus einer Arbeit von Daniel Micciancio ([17]). Der Satz führt die Schwierigkeit des Inc-GIVP$_\gamma^{n_\epsilon}$-Problems auf das GIVP$_\gamma^{n_\epsilon}$-Problem zurück. Er beweist dies über die von ihm selber eingeführten „Inkrementellen Reduktionen“. Wir geben einen direkte Polynomialzeitreduktion an, die sich eng an die Reduktion von Daniel Micciancio richtet.

Satz 4.17 *Es existiert eine Polynomialzeitreduktion von* Inc-GIVP$_\gamma^{n_\epsilon}$ *zu* GIVP$_\gamma^{n_\epsilon}$*, unter der Voraussetzung einer polynomiell beschränkten Eingabe in Abhängigkeit der Gitterdimension n. Das heißt, zu einem gewissen Polynom $p(x)$ werden nur Instanzen (B) des* GIVP$_\gamma^{n_\epsilon}$*-Problems betrachtet, für die $\|B\| \leq p(n)$ gilt.*

Beweis. Gegeben sei eine Instanz (B) mit $\|B\| \leq p(n)$ des GIVP$_\gamma^{n_\epsilon}$-Problems. Außerdem sei $\mathcal{O}$ ein Orakel, dass Inc-GIVP$_\gamma^{n_\epsilon}$ löst. Dann liefert folgender Algorithmus eine Reduktion:

RedIncGIVP$(B, \gamma, \eta_\epsilon) : \Lambda(B)^n$

1. Setze die Vektormenge S gleich der Basis B des Gitters:
$$S \leftarrow B$$
2. Sortiere die Vektoren in S aufsteigend nach ihrer Norm, und bezeichne diese mit $s_1, \ldots, s_n$, es gilt also $\max\limits_{i\in[n]} s_i = s_n$
3. Definiere die Hyperebene $\mathcal{H} = \text{span}\{s_1, s_2, \ldots, s_{n-1}\}$ und $S = \{s_1, \ldots, s_n\}$.
4. Führe das Orakel aus:
$$h \leftarrow \mathcal{O}(B, S, H)$$
5. Aktualisiere den Vektor s_n auf h
$$s_n \leftarrow h$$
6. Falls $\max\limits_{i\in[n]} \|s_i\| \leq \gamma \cdot \eta_\epsilon(\Lambda(B))$
output S, ansonsten springe zu 2.

In jedem Durchlauf gibt $\mathcal{O}$, falls $\|S\| \geq \gamma \cdot \eta_\epsilon(\Lambda(B))$ gilt, einen Vektor h zurück mit $\|h\| \leq \|S\|/2$. Gilt diese Ungleichung bricht der Algorithmus im letzten Schritt ab und liefert eine Lösung S des GIVP$_\gamma^{n_\epsilon}$-Problems. Wir betrachten die Parameter $(B, S^i = (s_1^i, \ldots, s_n^i), \mathcal{H}^i)$ im i-ten Durchlauf vor dem Ausführen des Orakels. Nach n weiteren Durchläufen erhalten wir mindestens eine Halbierung der Norm von $\|S\|$, dass heißt es gilt $\|S^{i+1}\| \leq \|S^i\|$, falls $\|S\|/2 \geq \gamma \cdot \eta_\epsilon(\Lambda(B))$. Sei nun $h^i \leftarrow \mathcal{O}(B, S, H)$. Dann erhalten wir im nächsten Durchlauf $S^{i+1} = (s_1^i, \ldots, s_{n-1}^i, h^i)$ vor dem Sortieren, mit

$\|h\| \leq \|S\|/2$. Im „schlechtesten“ Fall ist nun h^i der kleinste Vektor. Somit gilt nach dem Sortieren $S^{i+1} = (h^i, s_1^i, \ldots, s_{n-1}, h^i)$. Führen wir diesen Prozess iterativ weiter rückt mit jeder Iteration h^i in der Sortierung eine Position vor. Damit gilt, falls jeweils der „schlechteste “ Fall auftritt $S^{i+n} = (h^{i+1}, \ldots, h^{ni+})$ und damit ist $\|S^{i+n}\| \leq \|S\|/2$. Ist h^i in den jeweiligen Schritten nicht der kleinste Vektor, würde h^i gleich mehrere Positionen nach vorne rücken und der Prozess würde nur beschleunigt werden.
Damit wird der Wert $\|S\|$ alle n Durchläufe mindestens halbiert und wir erhalten dadurch eine Abschätzung für die maximale Durchlaufzahl t:

$$\begin{aligned} \frac{1}{2^{t/n}}\|B\| &\leq \gamma \cdot \eta_\epsilon(\Lambda(B)) \\ \Leftrightarrow t &\geq n \cdot \log\left(\frac{\|B\|}{\gamma \cdot \eta_\epsilon(\Lambda(B))}\right) \end{aligned}$$

Da $\|B\|$ nach Voraussetzung polynomiell beschränkt ist, liegt die maximale Durchlaufzahl t in Abhängigkeit von n im Raum $O(n^2)$. Damit läuft die Reduktion in Polynomialzeit und wir erhalten die gewünschte Aussage. ∎

Es fehlt nun noch ein Schritt, um die gewünschte Reduktionskette zu vervollständigen. Um das SIVP_γ-Problem auf $\text{GIVP}_\gamma^{n_\epsilon}$ reduzieren zu können, benötigt man die Abschätzung aus Lemma 3.9 des Glattheitparameters. Die Reduktion ergibt sich dann direkt aus dieser Ungleichung.

Lemma 4.18 *Es existiert eine Polynomialzeitreduktion von* $\text{GIVP}_\gamma^{n_\epsilon}$ *zu* SIVP'_γ, *mit* $\gamma' = \gamma \cdot \sqrt{\frac{\ln(2n(1+1/\epsilon))}{\pi}}$.

Beweis. Diese Reduktion ist trivial. Zu einem beliebigem Gitter Λ und dessen Basis B, wird das Orakel $\mathcal{O}$ zu $\text{GIVP}_\gamma^{n_\epsilon}$ aufgerufen und für $(h_1, \ldots, h_n) = \mathcal{O}(B)$ gilt dann durch Lemma 3.9 die gewünschte Aussage

$$\max_{i\in[n]}\|h_i\| \leq \gamma\eta_\epsilon(\Lambda) \leq \gamma \cdot \sqrt{\frac{\ln(2n(1+1/\epsilon))}{\pi}} \cdot \lambda_n(\Lambda) = \gamma' \cdot \lambda_n(\Lambda).$$

∎

4.3.2 Reduktion des SKS-Problems

Zu dem SKS-Problem lässt sich, analog zum M-SIS-Problem, eine worst-to-average-case-Reduktion angeben. Der einzige Unterschied ergibt sich in der Ziehung der y_l. Durch die Reduktion der Matrix A im SKS-Problem um d Dimensionen müssen nur $m - d$ Elemente aus der Normalverteilung $D_{\Lambda,s,0}$ gezogen werden. Zu einem Orakel $\mathcal{O}$ des SKS-Problems gibt folgender, leicht abgewandelter Algorithmus, eine Reduktion zum Mod-Inc-$\text{GIVP}_\gamma^{n_\epsilon}$-Problem an.

RedSKS$((B, S, H) : h \in \Lambda(B))$

1. Wähle t maximal, so dass ein s existiert mit:

$$\max\left(\frac{2q}{\gamma}, \sqrt{\log N}\right)\|S\| \leq s \leq \frac{q \cdot \|S\|}{2\beta\sqrt{N} \cdot t}$$

2. Ziehe aus der diskreten Normalverteilung $D_{\Lambda(B),s,c}$ mit dem Algr. SampleG:

$$y_l \xleftarrow{\$} \text{SampleG}(s, 0, B) \qquad \text{für } l = 1, \ldots, m-d$$

3. Führe $y_l \in \Lambda(B)$ auf R_q^d zurück mit dem Isomorphismus θ:

$$a_l \leftarrow \theta^{-1}(y_l \bmod qM) \qquad \text{für } l = 1, \ldots, m-d$$

4. Führe das Orakel $\mathcal{O}$ aus:

$$z_l \leftarrow \mathcal{O}(a_1, \ldots, a_m) \qquad \text{für } l = 1, \ldots, m$$

5. Berechne den Lösungsvektor h:

$$h \leftarrow \frac{1}{q}\sum_{l=1}^{d} z_l \cdot e_l + \sum_{l=d}^{m} z_l \cdot y_{l-d}$$

6. **Output** $\sigma(h)$.

Das Orakel löst somit das SKS-Problem zur Matrix

$$A = \begin{bmatrix} I_d & a_1 & \cdots & a_{m-d} \end{bmatrix}.$$

Dadurch ergeben sich analog die Reduktionssätze 4.19, 4.20 sowie eine Reduktionskette wie in Abbildung 4.

Satz 4.19 *Seien die Parameter gewählt wie in den Tabellen* 2 *und* 3. *Sei* $\mathcal{O}$ *ein Orakel, welches das* M-SIS$^2_{R_q^d,\beta,m}$ *Problem mit einer Wahrscheinlichkeit von* p *löst. Außerdem sei* ϵ' *die statistische Entfernung zwischen* SampleG$(s, 0, B)$ *und* $D_{\Lambda(B),s,0}$. *Dann löst RedMSIS das* Mod-Inc-GIVP$^{n_\epsilon}_\gamma$*-Problem mit einer Wahrscheinlichkeit* $\tilde{p}$ *von mindestens*

$$\tilde{p} \geq (p - 2(m-d)(\epsilon + \epsilon'))\left(\frac{1}{10} - \left(\frac{1+\epsilon}{1-\epsilon}\right)^{m-d} 2 \cdot N \cdot e^{-\pi t^2} - \epsilon'\right).$$

Satz 4.20 *Sei* $c > 1$. *Für alle* $d \geq 1$ *und* $\epsilon(N) = N^{-\omega(1)}$ *existiert eine probalistische Reduktion von* Mod-GIVP$^{n_\epsilon}_\gamma$ *zu* SKS$^2_{R_q^d,\beta,m}$ *mit einer nicht vernachlässigbaren Wahrscheinlichkeit für alle Parameter, die wie in den Tabellen 2 und 3 gewählt sind und folgende*

Ungleichungen erfüllen:

$$\gamma(N) \geq 4 \cdot \sqrt{\frac{c}{\pi}} \cdot \beta\sqrt{N} \cdot \sqrt{\log(N)} \tag{4.10}$$

$$q(N) \geq 2 \cdot \sqrt{\frac{c}{\pi}} \cdot \beta \cdot \sqrt{N} \cdot \log(N) \tag{4.11}$$

$$m, log(q) \leq poly(N) \tag{4.12}$$

Insbesondere besitzt die Reduktion eine polynomielle Laufzeit, falls das Orakel in polynomieller Zeit läuft.

Die Beweise laufen analog zu den Beweisen der Sätze 4.15 und 4.16 ab. Die Wahrscheinlichkeit von Satz 4.15 in der SKS-Variante wird dabei etwas verbessert, da SampleG d-mal seltener aufgerufen wird. Dies ist aber in der Praxis uninteressant, da die statitische Distanz ϵ' sehr klein und die Anzahl von Ziehungen m zumeist relativ klein ist.

4.4 Das LWE-Problem

„Learning with errors“ ist ein Problem aus der Komplexitätstheorie. Es wurde 2005 von Oded Regev eingeführt. Er bewies, dass sich die Sicherheit des LWE-Problems im durchschnittlichen Fall auf Gitterprobleme im schlechtesten Fall zurückführen lässt.

In diesem Kapitel werden die Entscheidungs- sowie Suchvariante des LWE-Problems sowie eine spezielle Variante des Modul-LWE-Problems beschrieben. Dafür wird eine Wahrscheinlichkeitsdichtefunktion χ über dem Segment $\mathbb{T} = \mathbb{R}/\mathbb{Z} \simeq [0, 1[$ benötigt. Zu einem Geheimnis $s \in \mathbb{Z}_q^n$, einer gleichverteilten Zufallsvariable $a \sim \mathrm{U}(\mathbb{Z}_q^n)$ sowie einem nach χ verteiltem Fehler e ergibt sich die Zufallsvariable $(a, \frac{1}{q}\langle a, s\rangle + e)$. Dadurch ergibt sich eine Verteilung über $\mathbb{Z}_q^n \times \mathbb{T}$. Diese wird fortan mit $A_{s,\chi}$ bezeichnet. Für die Probleme werden m Stichproben $(a_i, \frac{1}{q}\langle a_i, s\rangle + e_i)_{i\in[m]}$ betrachtet. Im Suchproblem soll zu den m Stichproben aus $A_{s,\chi}$ das Geheimnis s gefunden werden. Wir schreiben die Vektoren a_i als Zeilen in eine Matrix und bezeichnen diese fortan mit A.

$$A = [a_1| \dots |a_m]^T \in \mathbb{Z}_q^{m\times n}$$

Somit lässt sich das Such-LWE-Problem folgendermaßen definieren.

Definition 4.21 ($\mathbf{SLWE}^{\chi}_{n,q,\beta,m}$) Gegeben sei ein Geheimnis $s \in \mathbb{Z}_q^n$ sowie m unabhängige Ziehungen $(a_i, b_i)_{i\in[m]} \in \mathbb{Z}_q^n \times \mathbb{T}$ aus $A_{s,\chi}$, bezüglich dem Geheimnis s.
Finde das Geheimnis s.

Für Betrachtungen im durchschnittlichen Fall wird das Geheimnis aus einer Gleichverteilung über $\mathbb{Z}_q^n$ gezogen.

Beim Entscheidungsproblem dagegen betrachten wir die leicht abgewandelte Verteilung $A^D_{s,\chi}$. Sie gibt in 50% der Fälle m Stichproben aus $A_{s,\chi}$ zurück und in den anderen 50% gibt sie m Tupel der Form (a, u) zurück, mit den gleichverteilten Zufallsvariablen $u \sim \mathrm{U}(\mathbb{T})$ und $a \sim \mathrm{U}(\mathbb{Z}_q^n)$. Zu den m Stichproben aus $A^D_{s,\chi}$ soll nun entschieden werden ob diese aus $A_{s,\chi}$ oder aus der Gleichverteilung über $\mathbb{Z}_q^n \times \mathbb{T}$ stammen.

Definition 4.22 ($\mathbf{DLWE}^{\chi}_{n,q,\beta,m}$) Gegeben sei ein Geheimnis $s \in \mathbb{Z}_q^n$ sowie die m Ziehungen $(a_i, b_i)_{i\in[m]} \in \mathbb{Z}_q^n \times \mathbb{T}$ aus $A^D_{s,\chi}$, bezüglich dem Geheimnis s.
Ziel: Entscheide ob die Ziehungen aus $A_{s,\chi}$ oder aus der Gleichverteilungen stammen.

Bei dem in [1] definierten Decisional-Knapsack-Problem wird das Geheimnis und der Fehler aus der selben Gleichverteilung gezogen. Es handelt sich somit um das Modul-LWE-Problem in der Hermite-Normalform. Wir betrachten dafür einen Kreisteilungsring R, sowie den zugehörigen Faktorring $R_q = R/qR$, zu einer Primzahl q. Sei nun $\mathrm{U}(S_\beta)$ die Gleichverteilung über S^d_β. Sei $d \in \mathbb{N}$ die gewünschte Dimension des zugrundeliegenden Moduls und m wieder die Anzahl der Ziehungen. Das Geheimnis wird nun aus S^{d-m}_β gezogen und der Fehler wird jeweils aus $\mathrm{U}(S_\beta)$ gezogen. Damit ergeben sich durch $a_i \xleftarrow{\$} U(R_q^{d-m})$, für $i \in [m]$, die m Stichproben $(a_i, \langle a_i, s\rangle + e) \in R_q^d \times R_q$. Fassen wir wieder die m Ziehungen in Matrixschreibweise auf, dann erhalten wir $(A, A\cdot s+e) \in R_q^{m\times(d-m)} \times R_q^m$. Dies lässt sich umschreiben zu $(A, \begin{bmatrix} I_m & A \end{bmatrix} \cdot y)$ mit $y = (e^T, s^T)^T$. Mit $A_{y,\mathrm{U}(S_\beta)}$ bezeichnen wir ab sofort die dadurch entstehende Verteilung. Somit ergibt sich wieder die Verteilung $A^D_{y,\mathrm{U}(S_\beta)}$, die zu gleicher Wahrscheinlichkeit aus $(A, \begin{bmatrix} I_m & A \end{bmatrix} \cdot y)$ und (A, u) zieht, mit gleichverteiltem $u \sim U(R_q^m)$. Dann lässt sich das DKS-Problem im durchschnittlichen Fall folgendermaßen definieren.

Definition 4.23 ($\mathbf{DKS}_{R_q,d,\beta,m}$) Gegeben sei $y \xleftarrow{\$} R_q^d$ und $A \xleftarrow{\$} R_q^{m\times(d-m)}$, sowie $(A, b) \in R_q^{m\times(d-m)} \times R_q^m$, gezogen aus $A^D_{y,\mathrm{U}(S_\beta)}$. Entscheide aus welcher Verteilung (A, b) gezogen wurde.

Angenommen ein Angreifer $\mathcal{A}$ gibt $b = 0$ zurück, falls er sich für die Gleichverteilung entscheidet und ansonsten gibt er $b = 1$ zurück. Dann lässt sich der entstehende Vorteil eines Angreifers $\mathcal{A}$ folgendermaßen definieren.

Definition 4.24 (Vorteil $\mathbf{DKS}_{R_q,d,\beta,m}$) (vgl. [1],Definition 1)
Ein Angreifer $\mathcal{A}$ hat einen Vorteil von ϵ, falls

$$\Bigg|\mathrm{P}\left[b = 1 \mid A \xleftarrow{\$} R_q^{m\times(d-m)}, y \xleftarrow{\$} S_q^d, b \leftarrow \mathcal{A}(A, \begin{bmatrix} I_m & A \end{bmatrix} \cdot y)\right] -$$
$$\mathrm{P}\left[b = 1 \mid A \xleftarrow{\$} R_q^{m\times(d-m)}, u \xleftarrow{\$} R_q^m, b \leftarrow \mathcal{A}(A, u)\right]\Bigg| \geq \epsilon$$

gilt.

5 Das Commitment-Verfahren

In diesem Kapitel wird das in [1] beschriebene Commitment-Verfahren beschrieben und zu gewissen Parametern analysiert, um genaue Sicherheitsaussagen zu bekommen.

5.1 Der Challenge-Raum

Es wurden bisher oft Kreisteilungsringe mit 2er Potenz betrachtet. Dies liegt daran, dass dort kleine Ringelemente stets invertierbar sind. Der Raum der diese Elemente enthält wird Challenge-Raum genannt. Dieser Raum wird benötigt, um die Soundness-Eigenschaft des zugrunde liegenden Zero-Knowledge-Protokolls zu beweisen. Auf das Zero-Knowledge-Protokoll wird in dieser Arbeit nicht eingegangen, aber der Challenge-Raum taucht auch in den Reduktionen zur Binding-, sowie Hiding-Eigenschaft auf und wird deshalb in diesem Kapitel angesprochen. Folgendes Lemma aus [18] bildet die Grundlage des Challenge-Raums.

Lemma 5.1 ([18], Corollary 1.2) *Seien $n \geq k > 1$ 2-er Potenzen und $p = 2k + 1 (\mathrm{mod}\ 4k)$ eine Primzahl. Dann zerfällt das Polynom $X^n + 1$ in k irreduzible Polynome $X^{n/k} - r_j \bmod q$. Außerdem ist jedes $y \in R_q \setminus \{0\}$ für dass entweder*

$$\|y\|_\infty \leq \frac{1}{\sqrt{k}} \cdot q^{1/k} \qquad oder \qquad \|y\|_2 \leq q^{1/k}$$

gilt invertierbar in R_q.

Durch dieses Lemma liegen im Challenge-Raum

$$\mathcal{C} := \{c \in R_q \mid \|c\|_\infty = 1, \|c\|_1 = \kappa\|\}$$

nur invertierbare Elemente, falls der Kreisteilungsring $R_q = \mathbb{Z}[X]_q / \langle X^n + 1 \rangle$ gewählt wurde wie in Lemma 5.1. Der Parameter κ dient dazu, die Größe(Anzahl der Elemente) des Challenge-Raums festzulegen. Soll der Challenge-Raum 2^λ Elemente beinhalten, so wird κ so klein wie möglich gewählt, sodass $\left\{ {N \atop \kappa} \right\} \cdot 2^\kappa > 2^\lambda$ gilt. Außerdem wird der Raum der Differenzen aus $\mathcal{C}$ folgendermaßen definiert

$$\bar{\mathcal{C}} = \{c - c' \mid c \neq c' \in \mathcal{C}\}$$

5.2 Definition des Commitment-Verfahrens

Im Folgenden definieren wir das Commitment-Verfahren über das Tupel $(\mathrm{gen}, \mathrm{com}, \mathrm{open})$ von Algorithmen in Abhängigkeit des Sicherheitsparameters η. Das Commitment-Verfahren lässt sich zu einem Kreisteilungsring R und Parametern definieren wie sie Tabelle 4 stehen. Im Vergleich zu [1] wurden die Parameter anders benannt, um ein besseres Zusammenspiel mit den Parameternamen der Probleme zu erhalten. Für den Leser, der die Parameter mit denen aus [1] vergleichen möchte, sieht die entsprechende Bezeichnung aus [1] in der

4. Spalte von Tabelle 4.

Parameter	**Beschreibung**	**Typ**	vgl. [1]
n	Dimension des Kreisteilungsrings (2er-Potenz)	$\in \mathbb{N}$	N
q	Restklassenparameter	$\in \mathbb{N}$	q
k	2er Potenz benötigt für Invertibilität des Challenge-Raums	$\in \mathbb{N}$	d
m	Breite der Commitment-Matrix (über R_q)	$\in \mathbb{N}$	k
h	Höhe der Commitment-Matrix (über R_q)	$\in \mathbb{N}$	n
l	Dimension des Nachrichtenraums (über R_q)	$\in \mathbb{N}$	l
β	(Maximums)-Normgrenze des Zufalls r	$\in \mathbb{R}_+$	β
κ	Maximale Summennorm von Elementen aus $\mathcal{C}$	$\in \mathbb{R}_+$	κ
$\sigma = 11\kappa \cdot \beta \cdot \sqrt{mn}$	Hilfsparameter zur Überprüfung der Länge des Zufalls r in open	$\in \mathbb{R}_+$	σ

Tabelle 4: Parameter zum Commitment-Verfahren

Mit PAR $= (n, q, m, h, l, \beta, \kappa, \sigma)$ bezeichnen wir ab sofort Parameter, die gewählt sind wie in der obigen Tabelle. Zudem nehmen wir an, dass k, q, n so gewählt sind wie in Lemma 5.1, damit der Challenge-Raum nur invertierbare Elemente enthält. Im folgenden definieren wir das Commitment-Verfahren zu solchen Parametern PAR. Nachrichten x liegen im Nachrichtenraum R_q^l und Commitments c liegen im Raum R^{h+l}. Die Zufallsgröße r wird aus der Menge S_β^m gezogen. Der probalistische Algorithmus gen_{PAR} gibt Matrizen A_1 und A_2 über dem Kreisteilungsring R zurück.

Gen$_{\text{PAR}}() : R_q^{(h+l)\times m} \times R_q^{l\times m}$

1. Generiere Matrix A_1:

$$A_1' \xleftarrow{\$} R_q^{h\times(m-h)} \qquad A_1 \leftarrow \begin{bmatrix} I_h & A_1' \end{bmatrix}$$

2. Generiere Matrix A_2:

$$A_2' \xleftarrow{\$} R_q^{l\times(m-h-l)} \qquad A_2 \leftarrow \begin{bmatrix} 0^{l\times h} & I_l & A_2' \end{bmatrix}$$

3. **output** $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$

Zu festen öffentlichen Parametern $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$ lassen sich nun die Algorithmen **Com** und **Open** definieren. Der Algorithmus **Com** gibt zu einer gegebenen Nachricht x ein Commitment zurück, welches ein Vektor aus dem Ring R_q^{h+l} darstellt.

$\mathbf{Com}(x \in \mathcal{R}_q^l) : \mathcal{R}_q^{h+l}$

1. Generiere den Zufallsvektor r:
$$r \xleftarrow{\$} S_\beta^m$$
2. Berechne das Commitment zu der Nachricht x und dem Zufall r:
$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \leftarrow \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \cdot r + \begin{bmatrix} 0^h \\ x \end{bmatrix}$$
3. **output** c

Der deterministische Algorithmus open überprüft ob das Tupel (x, r, f) zu dem gegebenen Commitment c passt.

$\mathbf{Open_c}(x \in \mathcal{R}_q^l, r \in R_q^m, f \in \bar{\mathcal{C}}) : \{0, 1\}$

1. Überprüfe ob
$$f \cdot \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \cdot r + f \cdot \begin{bmatrix} 0^h \\ x \end{bmatrix} \qquad \text{gilt.}$$
2. Überprüfe ob
$$\|r_i\|_2 \leq 4\sigma\sqrt{n} \qquad \text{gilt.}$$
3. Falls 1. und 2. gilt,
outpout 0, ansonsten **output** 1

5.3 Reduktion der Binding-Eigenschaft

In diesem Kapitel führen wir die Binding-Eigenschaft des Commitment-Verfahrens auf die Sicherheit des worst-case-Mod-GIVP$_\gamma^{n_\epsilon}$-Problems zurück. Dafür wird zuerst eine Reduktion wie in [1] angegeben, um die Sicherheit der Binding-Eigenschaft auf das SKS-Problem zurückzuführen.

Lemma 5.2 (vgl:[1],Lemma 7) *Falls es einen Algorithmus $\mathcal{A}$ gibt der die Binding-Eigenschaft mit einem Vorteil von p bricht, dann existiert ein Algorithmus $\mathcal{A}'$, der das* SKS$^2_{R_q^h, 16\sigma\sqrt{\kappa n}, m}$*-Problem mit gleichem Vorteil p löst(im Durchschnittsfall). Insbesondere ist die Laufzeit von $\mathcal{A}'$ polynomiell in N, falls die Laufzeit von $\mathcal{A}$ polynomiell in N ist.*

Beweis. Zu einer Instanz $A_1' \in R_q^{h \times (m-h)}$ des SKS$^2_{R_q^h, 16\sigma\sqrt{\kappa n}, m}$-Problems lässt sich der Algorithmus $\mathcal{A}'$, der das SKS$^2_{R_q^h, 16\sigma\sqrt{\kappa n}, m}$-Problem löst mit Hilfe des Algorithmus $\mathcal{A}$ direkt angeben:

$\mathcal{A}'(A'_1 \in R_q^{h\times(m-h)}) : h \in R_q^m$

1. Generiere eine Matrix A_2, wie in gen_{PAR}:

$$A'_2 \xleftarrow{\$} R_q^{l\times(m-h-l)} \qquad A_2 = \begin{bmatrix} 0^{l\times h} & I_l & A'_2 \end{bmatrix}$$

2. Führe den Algorithmus $\mathcal{A}$ aus:

$$(x, r, f, x', r', f', c) \leftarrow \mathcal{A}(\begin{bmatrix} I_h & A'_1 \end{bmatrix}, A_2)$$

3. Output h $\leftarrow f' \cdot r - f \cdot r'$

Da wir die Komplexität von $\mathcal{A}'$ im durchschnittlichen Fall betrachten, wählen wir $A'_1 \xleftarrow{\$} R_q^{h\times(m-h)}$. Wir interessieren uns für den Erfolg von $\mathcal{A}'$. Dazu betrachten wir die Zufallsvariable $h = \mathcal{A}'_{A'_2}(A'_1)$. Diese gibt in Abhängigkeit der Zufallsvariablen A'_1 und A'_2 die Ausgabe des Algorithmus $\mathcal{A}'$ an. Die Zufallsvariablen A_1 und A_2 sind gleich verteilt wie im Algorithmus gen_{PAR}. Damit gibt $\mathcal{A}$ mit einer Wahrscheinlichkeit von $p = \text{P}\left[\mathbb{E}_A^{binding} = 1\right]$ das Tupel (x, r, f, x', r', f', c) mit der Eigenschaft $\text{open}_c(x, r, f) = 1 = \text{open}_c(x', r', f')$ zurück und somit gilt

$$f \cdot \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \cdot r + f \cdot \begin{bmatrix} 0^h \\ x \end{bmatrix} \tag{5.1}$$

$$f' \cdot \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \cdot r' + f' \cdot \begin{bmatrix} 0^h \\ x' \end{bmatrix} \tag{5.2}$$

$$\|r'_i\|, \|r_i\| \leq 4\sigma\sqrt{n} \qquad \text{für alle } i \in [m]. \tag{5.3}$$

Wir multiplizieren (5.1) mit f' und (5.2) mit f und subtrahieren die Gleichungen, wodurch wir folgende Gleichungen erhalten:

$$A_1 \cdot (f' \cdot r - f \cdot r') = 0 \tag{5.4}$$

$$A_2 \cdot (f' \cdot r - f \cdot r') + (f \cdot f' \cdot (x - x')) = 0. \tag{5.5}$$

Da f und f' Elemente der Menge $\bar{\mathcal{C}}$ sind, sind diese invertierbar und somit ist $f \cdot f'$ kein Nullteiler. Damit gilt $f \cdot f' \cdot (x - x') \neq 0$ und somit muss auch $(f' \cdot r - f \cdot r')$ ungleich Null sein. Wir erhalten somit insgesamt durch die Ungleichungen $\|f\|_2, \|f'\|_2 \leq 2\sqrt{\kappa}$, der Gleichung (5.3), sowie den Abschätzungen (2.10) und (2.12) die Ungleichung

$$\|h\| = \|f' \cdot r - f \cdot r'\| \leq \|f'\|_2 \cdot \|r\|_2 + \|f\|_2 \cdot \|r'\|_2 = 16\sigma\sqrt{m \cdot n}$$

und somit löst $\mathcal{A}'$ das $\text{SKS}^2_{R_q^h, 16\sigma\sqrt{\kappa n}, m}$-Problem mit Wahrscheinlichkeit p. ∎

Nun kann mit Hilfe von Kapitel 4.3 eine Reduktion zum Mod-$\text{GIVP}^{n_\epsilon}_\gamma$-Problem angegeben werden. Es ergibt sich somit eine Reduktionskette(s. Abb. 6), wie in Kapitel 4.3. Im folgenden Satz betrachten wir das Commitment-Verfahren zu dem Sicherheitspara-

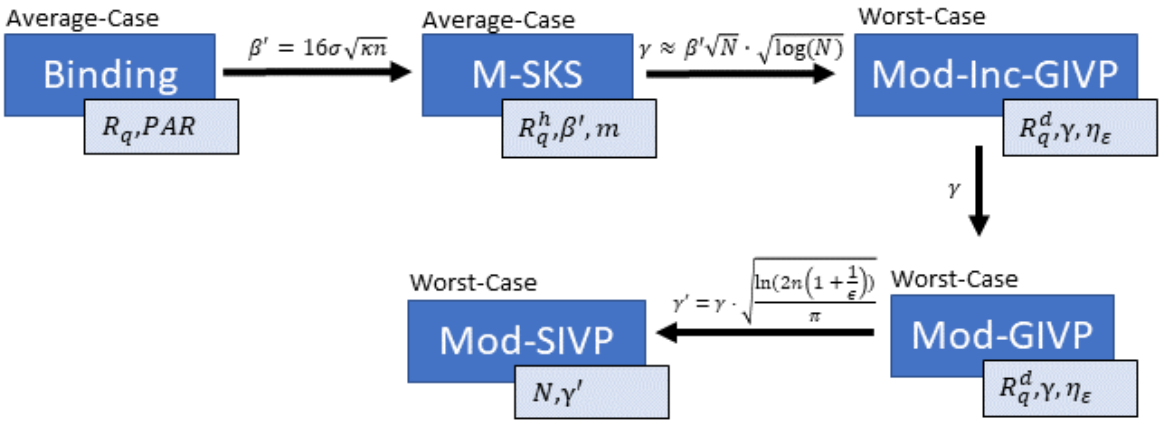

Abbildung 6: Reduktionskette - Binding - Mod-GIVP

meter $N = n \cdot h$, der sich aus der Dimension des Kreisteilungsrings und der Höhe der Commitment-Matrix zusammensetzt. Die anderen Parameter werden in Abhängigkeit von diesem gewählt.

Satz 5.3 *Gegeben seien Parameter (q, m, l, β) in Abhängigkeit von $N = nh$. Außerdem sei κ gewählt wie in Kapitel 5.1 und $\sigma(N) = 11\kappa \cdot \beta(N)\sqrt{m(N) \cdot n}$. Gilt*

$$q(N) \geq 2 \cdot \sqrt{\frac{c}{\pi}} \cdot 16\sigma\sqrt{\kappa n} \cdot \sqrt{N} \cdot \log(N)$$
$$m, log(q) \leq poly(N)$$

für ein $c > 1$, dann erhalten wir zu $\epsilon = N^{-\omega(1)}$ und dem Approximationsfaktor

$$\gamma(N) = 4 \cdot \sqrt{\frac{c}{\pi}} \cdot 16\sigma\sqrt{\kappa n} \cdot \sqrt{N} \cdot \sqrt{\log(N)} \cdot \sqrt{\frac{\ln(2N(1+1/\epsilon))}{\pi}}$$

folgende Aussage: Falls es einen Algorithmus $\mathcal{A}$ gibt der die Binding-Eigenschaft mit einem Vorteil von p bricht, dann existiert ein Algorithmus $\mathcal{A}'$ der das $\mathrm{SIVP}_{\gamma'}$-Problem(eingeschränkt auf Modul-Gitter) mit überwältigender Wahrscheinlichkeit p' löst. Außerdem ist die Laufzeit von $\mathcal{A}'$ polynomiell in N, falls die Laufzeit von $\mathcal{A}$ polynomiell in N ist.

Beweis. Der Beweis ergibt sich direkt durch die Reduktionskette aus Kapitel 4.3, sowie Lemma 5.2. ∎

Wählt man $\epsilon = N^{-\sqrt{\log(N)}}$ so erhält durch den letzten Satz einen asymptotischen Approximationsfaktor von

$$\gamma(N) = O\left(\beta(N)\sqrt{m(N)} \cdot n \cdot \sqrt{N}\log(N)\sqrt{\log(N)}\right).$$

Dabei fällt der Parameter κ raus, da dieser, wie in Kapitel 5.1 gewählt, mit steigendem N kleiner wird. Nimmt man an, dass die Dimension des Kreisteilungskörpers n linear mit N wächst, so erhält man den Approximationsfaktor

$$\gamma(N) = O\left(\beta(N)\sqrt{m(N)} \cdot (\log(N) \cdot N)^{3/2}\right). \tag{5.6}$$

Wählt der Algorithmus zum Erzeugen der öffentlichen Parameter gen(N) Parameter in Abhängigkeit von N, sodass die Voraussetzungen von Satz 5.3 erfüllt sind, dann beruht die Binding-Eigenschaft des Commitment-Verfahrens auf dem Mod-SIVP$_\gamma$-Problem, mit einem Approximationsfaktor $\gamma(N)$ wie in Gleichung (5.6).

5.4 Reduktion der Hiding-Eigenschaft

Der Beweis des nachfolgenden Lemmas entspricht im Wesentlichen dem aus [1]. Wir passen den Beweis strukturell an, um eine ähnliche Struktur zur Sicherheitsdefinition der Hiding-Eigenschaft aus Kapitel 2.1.1 zu bekommen.

Lemma 5.4 (vgl. [1],Lemma 6) *Falls es einen Algorithmus $\mathcal{A}$ gibt der die Hiding-Eigenschaft mit einem Vorteil von ϵ bricht, dann existiert ein Algorithmus $\mathcal{A}'$, der das* DKS$_{m,\beta,h+l}$*-Problem mit dem gleichem Vorteil ϵ löst. Insbesondere ist die Laufzeit von $\mathcal{A}'$ polynomiell in N, falls die Laufzeit von $\mathcal{A}$ polynomiell in N ist.*

Beweis. Zu einer Instanz $(B', t) \in R_q^{(h+l)\times(m-(h+l))} \times R_q^m$ des DKS-Problems geben wir den Algorithmus $\mathcal{A}'$, der das DKS-Problem löst, direkt an. Dazu sei $B = \begin{bmatrix} I_{h+l} & B' \end{bmatrix}$.

$\mathcal{A}'(B \in R_q^{(h+l)\times m}, t \in R_q^m) : h \in R_q^m$

1. Generiere öffentliche Parameter:

$$A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \leftarrow \begin{bmatrix} \mathrm{I}_h & R \\ 0 & \mathrm{I}_l \end{bmatrix} \cdot B, \qquad \text{mit } R \xleftarrow{\$} R_q^{h\times l}$$

2. Erhalte durch $\mathcal{A}_F$ „angreifbare“ Nachrichten:

$$x_0, x_1 \xleftarrow{\$} \mathcal{A}_F(A)$$

3. Wähle zufällig eine Nachricht und ein zugehöriges Commitment, mit dem „Zufall“ t aus:

$$b \xleftarrow{\$} \{0,1\}, \qquad c = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \leftarrow \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \cdot t + \begin{bmatrix} 0^h \\ x_b \end{bmatrix}$$

4. Führe $\mathcal{A}_G$ mit dem Commitment c aus:

$$b' \xleftarrow{\$} \mathcal{A}_G(A, c)$$

5. Auswertung: **if** $b' = b$ **output** 1, **else output** 0

Damit der Vorteil des Algorithmus $\mathcal{A}$ ausgenutzt werden kann zeigen wir als erstes, dass die Matrix A aus dem ersten Schritt der Reduktion gleich verteilt ist wie die Commitment-Matrix im Algorithmus $\text{gen}_{\text{PAR}}()$. Dazu wird B folgendermaßen umgeschrieben:

$$B = \begin{bmatrix} \mathrm{I}_h & 0 & B'_1 \\ 0 & \mathrm{I}_l & B'_2 \end{bmatrix}.$$

Somit ergibt sich

$$\begin{bmatrix} \mathrm{I}_h & R \\ 0 & \mathrm{I}_l \end{bmatrix} \cdot \begin{bmatrix} \mathrm{I}_h & 0 & B'_1 \\ 0 & \mathrm{I}_l & B'_2 \end{bmatrix} = \begin{bmatrix} \mathrm{I}_h & R & B'_1 + R \cdot B'_2 \\ 0 & \mathrm{I}_l & B'_2 \end{bmatrix} = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}.$$

Die Matrizen B'_1, B'_2 und R sind stochastisch unabhängig und gleichverteilt. Damit erkennt man an der letzten Gleichung, dass A aus $\mathcal{A}'(B)$, zu einem gleichverteilten B', der Verteilung aus $\text{gen}_{\text{PAR}}()$ entspricht. Nun werden zwei Fälle unterschieden:

1. Fall: t stammt aus der Gleichverteilung: Dann ist das durch $\mathcal{A}'$ erzeugt Commitment c ebenfalls gleichverteilt und somit insbesondere unabhängig von der gewählten Nachricht x_b. Somit ist der Vorteil von $\mathcal{A}'$ in diesem Fall genau $\frac{1}{2}$.

2. Fall: t stammt aus der Verteilung $A_{y,\mathrm{U}(S_\beta)}$, das heißt es gilt $t = By$ für das Geheimnis $y \in S_\beta$. In diesem Fall entspricht das c dem Commitment aus unserem Commitment-Verfahren. Durch Voraussetzung hat $\mathcal{A}$ einen Vorteil von $\frac{1}{2} + \epsilon$. Deshalb gilt mit einer Wahrscheinlichkeit von mindestens $\frac{1}{2} + \epsilon$ $b' = b$ und damit gibt $\mathcal{A}'$ mit dieser Wahrscheinlichkeit den Wert 1 zurück.

Somit gilt insgesamt

$$\Bigg| \mathrm{P}\left[b = 1 \mid B' \xleftarrow{\$} R_q^{(h+l)\times(m-(h+l))}, y \xleftarrow{\$} S_q^m, b \leftarrow \mathcal{A}(B', \begin{bmatrix} I_{h+l} & B' \end{bmatrix} \cdot y)\right] -$$
$$\mathrm{P}\left[b = 1 \mid B' \xleftarrow{\$} R_q^{(h+l)\times(m-(h+l))}, u \xleftarrow{\$} R_q^{h+l}, b \leftarrow \mathcal{A}(B', u)\right] \Bigg| \geq \frac{1}{2} + \epsilon - \frac{1}{2} = \epsilon$$

und damit die Aussage. ∎

5.5 Angriffe

In diesem Kapitel wird der triviale Angriff auf die Binding-Eigenschaft und der Dual-Anriff auf die Hiding-Eigenschaft beschrieben. Hierbei wird ähnlich vorgegangen, wie in den von Rachel Paper beschriebenen Angriffen([15]).

5.5.1 Angriff auf die Hiding-Eigenschaft

Der folgende Angriff ist eine Adaption des in [15] aufgeführten Dual-Angriffs für LWE-Instanzen. Der Angriff führt das LWE-Problem auf eine SIS-Instanz zurück und löst diese mithilfe von Gitter-Reduktions-Verfahren. Wir betrachten nun das $\text{DKS}_{R_q,d,\beta,m}$-Problem zu den Parametern $\beta \in \mathbb{R}_+, d, m \in \mathbb{N}$ und einem Kreisteilungsring mit 2er Potenz.

Gegeben sei eine Instanz $(A', b') \in R_q^{m\times(d-m)} \times \mathbb{R}_q^m$ des DKS-Problems. Wir fassen nun A' als Matrix über $\mathbb{Z}_q$ auf: $A = \mathrm{Rot}(A') \in \mathbb{Z}_q^{mn\times(d-m)n}$, wie in Kapitel 2.2.2. Somit erhalten wir ein LWE-Problem in dem der Fehler und das Geheimnis aus der Gleichverteilung über S_β gezogen werden. Eine Stichprobe $(A', \begin{bmatrix} I_m & A' \end{bmatrix} \cdot y)$ lässt sich mit Hilfe der Einbettung σ_{pol} folgendermaßen schreiben:

$$\sigma_{pol}(\begin{bmatrix} I_m & A' \end{bmatrix}) \cdot y = A \cdot s + e, \qquad \text{wobei } y = \begin{bmatrix} \sigma_{pol}(s) \\ \sigma_{pol}(e) \end{bmatrix}, e \in \mathbb{Z}_q^{nm}, s \in \mathbb{Z}_q^{(d-m)n}$$

Deshalb betrachten wir fortan die Instanz (A, b), mit $b = \sigma_{pol}(b')$. Die nächsten Schritte folgen dem Angriff aus Kapitel 4.6 in [15] mit dem Unterschied, dass wir einen gleichverteilten Fehler betrachten. Um entscheiden zu können, zu welcher Verteilung die Instanz gehört, betrachten wir den Kern von A. (vgl. Kapitel 3.1.1).

$$G_q(A)^\perp = \{v \in \mathbb{Z}_q^{mn} \mid vA = 0 \mod q\}$$

Wie in Kapitel 3.1.1 beschrieben entspricht es dem skalierten dualen Gitter bezüglich dem von A erzeugten Gitter $G_q(A)$. Finden wir nun einen kleinen Vektor v aus $G_q(A)^\perp$, erhalten wir durch das Betrachten des Skalaprodukts $\langle v, b\rangle$ einen Vorteil zum Lösen des DKS-Problems. Denn stammt b nicht aus der Gleichverteilung, dann gilt $b = A \cdot s + e$ für ein unbekanntes Geheimnis s und einem unbekannten Fehler e. Damit folgt durch die Wahl von v:

$$\langle v, b\rangle = \langle v, A \cdot s + e\rangle = v \cdot A + \langle v, e\rangle = \langle v, e\rangle.$$

Die Vektoren v und e sind klein, wodurch auch das Skalarprodukt klein ist. Auf der anderen Seite ist die Verteilung des Skalarprodukts $\langle v, b\rangle$, für die gleichverteilte Zufallsvariable b, wieder gleichverteilt. Dadurch ergeben sich, falls v klein genug gewählt worden ist, unterschiedliche Verteilungen. Außerdem lässt sich das duale Gitter $G_q(A)^\perp$, falls die Matrix A vollen Rang hat, durch folgende Basis darstellen([15],Kapitel 4.6):

$$\begin{bmatrix} \mathrm{I}_{mn-(d-m)n} & B' \\ 0 & q\mathrm{I}_{(d-m)n} \end{bmatrix}$$

Wir erhalten somit mit hoher Wahrscheinlichkeit $\mathrm{vol}(\Lambda) = q^{(d-m)n}$. Das Ziel ist also einen kleinen Vektor v zu finden, für den $vA = 0$ gilt. Dies entspricht gerade der Aufgabenstellung des SIS-Problems. Der Satz 5.6 besagt wie gut ein Gitter-Reduktionsverfahren sein muss, damit wir einen gewissen Vorteil erhalten.

Lemma 5.5 *Gegeben seien die Zufallsvariablen $u \sim \mathrm{U}(\mathbb{Z}_q^n)$ und $y \sim \mathrm{U}(S_\beta^n)$. Für $v \in \mathbb{Z}_q$ mit $\|v\|_1 \leq \frac{q}{2\beta}$. Dann lassen sich die Verteilungen $\langle v, u\rangle$ und $\langle v, y\rangle$ mit einem Vorteil von mindestens $\epsilon = \frac{q-2\beta\|v\|_1}{q}$ unterscheiden.*

Beweis. Durch die Voraussetzungen des Lemmas und einer Standardabschätzung des Skalarprodukts kann die Zufallsvariable $\langle v, y\rangle$ im Betrag maximal den Wert $\beta \cdot \|v\|_1$ annehmen. Insbesondere nimmt die Zufallsvariable $\langle v, y\rangle$ die Werte $-\frac{q}{2}, -\frac{q}{2}+1, \ldots, \frac{q}{2}-s$ sowie $\frac{q}{2}-s, \frac{q}{2}-s+1, \ldots, \frac{q}{2}$ nicht an, für $s = q/2 - \beta\|v\|_1$. Somit ergibt sich offensichtlich ein Vorteil in diesen $2s$ Fällen und somit von $\epsilon = \frac{2s}{q} = \frac{q-2\beta\|v\|_1}{q}$. ∎

Satz 5.6 *Sei $c \in \mathbb{N}$. Jedes Gitter-Reduktionsverfahren, das einen log-root-Hermite Faktor von*

$$\log(\delta_0) = \frac{\log(\frac{1}{\beta\sqrt{nm}}(\frac{q}{2} - c)) - \frac{d-m}{m}\log q}{nm}$$

erreicht, führt zu einem Vorteil von mindestens $\epsilon = \frac{c}{q/2}$ für das $\mathrm{DKS}^2_{R_q,d,\beta,m}$ Problem.

Beweis. Sei (A, b) eine Stichprobe des $\mathrm{DKS}^\infty_{R_q,d,\beta,m}$-Problems. Durch die Definition des Hermite-Faktors erhalten wir durch das GRV zu einem beliebigen Gitter $\Lambda \subset \mathbb{R}_{nm}$ einen Vektor v mit

$$\|v\|_2 = \delta_0^{nm} \cdot \mathrm{vol}(L)^{1/nm}.$$

Das Gitter $(G_q(A)^\perp$ hat mit hoher Wahrscheinlichkeit p ein Volumen von $q^{(d-m)n}$, was ab nun angenommen wird. Damit erhalten wir mit dem GRV einen Vektor v mit

$$\|v\|_2 = \delta_0^{nm} \cdot q^{(d-m)/m}.$$

und somit folgt durch Umformung der Gleichung:

$$\log(\delta_0) = \frac{\log\|v\|_2 - \frac{d-m}{m}\log q}{nm}.$$

Wählen wir $2c = q - 2\beta \cdot \sqrt{nm}\|v\|_2$ dann erhalten wir durch Lemma 5.5 und der Standardabschätzung der Summennorm den gewünschten Vorteil von mindestens $\epsilon = \frac{2c}{q}$. Durch einsetzten in die letzte Gleichung folgt damit die Aussage. ∎

5.5.2 Anriff auf die Binding-Eigenschaft

Wie im Beweis von Lemma 5.2 beschrieben, kann durch eine Reduktion die Sicherheit der Binding-Eigenschaft direkt auf die Schwierigkeit des SKS-Problems zurückgeführt werden. Diese Reduktion lässt sich auch umgekehrt formulieren. Wir betrachten das Commitment-Verfahren zu beliebigen Parametern PAR. Seien nun öffentliche Parameter $A = (A_1, A_2) \in R_q^{h\times m} \times R_q^{l\times m}$ gegeben. Angenommen wir finden ein $y \in R_q^m$ mit

$$A_1 y = 0 \text{ und } \|y\|_2 \leq 4\sigma\sqrt{n},$$

dann ist das Tupel $(x = -A_2 y, r = y, f = 1, x' = 0^l, r' = 0^m, f' = 1, c = 0^{l+h})$ ein zweideutiges Commitment, das die Binding-Eigenschaft bricht, denn es gilt

$$\begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \cdot y + \begin{bmatrix} 0^h \\ x \end{bmatrix} = \begin{bmatrix} 0^h \\ -x \end{bmatrix} \cdot y + \begin{bmatrix} 0^h \\ x \end{bmatrix} = 0^{l+h} = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}.$$

Falls $x = -A_2 y$ ungleich 0 ist, sind die Vektoren x und x' verschieden, womit das obige Tupel ein gültiges zweideutiges Commitment ist. Da die Matrizen A_1 und A_2 gleichverteilt und unabhängig voneinander sind, kann mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass $x \neq 0$ gilt. Dies liefert eine umgekehrte Reduktion zu Lemma 5.2 und insbesondere einen möglichen Angriff. Wie im vorherigen Kapitel beschrieben, kann das

SKS-Problem A_1 direkt über Gitter-Reduktions-Verfahren gelöst werden. Dazu wird wieder die Multiplikation in R_q durch die Einbettung σ_{pol} als Multiplikation in $\mathbb{Z}_q^n$ geschrieben, durch die Matrix $\mathrm{Rot}(A_1) \in \mathbb{Z}^{hn \times mn}$. Es wird also ein $y \in \mathbb{Z}_q^{nm}$ gesucht, für das

$$\mathrm{Rot}(A_1) \cdot y = 0 \text{ und } \|y\|_2 \leq 4\sigma\sqrt{n} \tag{5.7}$$

gilt. Nun betrachten wir, wie im letzten Kapitel das Gitter, welches durch den Kern von $\mathrm{Rot}(A_1)^T$ erzeugt wird:

$$G_q(\mathrm{Rot}(A_1)^T)^\perp = \{v \in \mathbb{Z}_q^{mn} \mid \mathrm{Rot}(A_1) \cdot v = 0 \mod q\}.$$

Da A_1 in Hermite-Normal-Form gegeben ist, hat A_1 und somit $\mathrm{Rot}(A_1)$ vollen Rang und es gibt eine Basis bezüglich der rechten Seite des Kerns von A_1, die $(mn - hn)$ Vektoren besitzt. Somit existiert die Basis

$$\begin{bmatrix} \mathrm{I}_{mn-hn} & B' \\ 0 & q\mathrm{I}_{hn} \end{bmatrix}$$

von $G_q(\mathrm{Rot}(A_1)^T)^\perp$ und das Volumen dieses Gitters beträgt

$$\mathrm{vol}(G_q(A_1^T)^\perp) = q^{hn}. \tag{5.8}$$

Durch diese Überlegungen lässt sich folgender Satz beweisen.

Satz 5.7 *Jedes Gitter-Reduktionsverfahren, welches einen log-root-Hermite Faktor von*

$$\log(\delta_0) = \frac{\log(4\sigma\sqrt{n}) - \frac{h}{m}\log q}{mn}$$

erreicht, bricht die Binding-Eigenschaft des Commitment-Verfahrens.

Beweis. Gegeben seien öffentlichen Parameter $A' = (A'_1, A'_2)$ des Commitment-Verfahrens. Sei $A_1 = \mathrm{Rot}(A_1)$. Dann kann durch den Vektor $y \in \mathbb{Z}_q^{nm}$, der die Bedingung (5.7) erfüllt, ein doppeldeutiges Commitment konstruiert werden. Wir wenden also das GRV auf das mn-dimensionale Gitter $G_q(A_1^T)^\perp$ an und erhalten somit durch (5.8) und der Definition des Hermite-Faktors:

$$\log(\delta_0) = \frac{\log \|y\|_2 - \frac{h}{m}\log q}{mn}.$$

Mit $\|y\|_2 = 4\sigma\sqrt{n}$ erhalten wir die Aussage. ∎

5.6 Analyse zu gewissen Parametern

In [1] werden Parameter angegeben zu denen das Commitment-Verfahren gute Sicherheitsergebnisse liefert(Tab. 5).

Parameter	**„Optimaler Wert“**
n	1024
q	$\approx 2^{32}$
k	2,4 oder 8
m	3
h	1
l	1
β	1
κ	36
$\sigma = \kappa \cdot \beta \cdot \sqrt{mn}$	≈ 27000

Tabelle 5: Optimale Parameter aus [1]

Unsere angegebenen Angriffe auf die Binding-Eigenschaft, sowie auf das DKS-Problem, welches mit der Sicherheit der Hiding-Eigenschaft zusammenhängt, bestätigen dies(Tab. 6). Die Parameter liefern allerdings keine worst-to-average-case-Reduktion der Binding-Eigenschaft bezüglich der Reduktion aus Kapitel 4.3.2. Dies wird im folgenden erläutert. Nach Lemma 5.2 basiert die Binding-Eigenschaft auf dem $\mathrm{SKS}^2_{R_q^h,16\sigma\sqrt{\kappa n},m}$-Problem. Durch die Wahl der Parameter lässt sich der Hilfsparameter t nach oben beschränken:

$$\begin{aligned} t =& \min\left(\frac{\gamma}{2\cdot 16\sigma\sqrt{\kappa n}\sqrt{n}}, \frac{q}{2\cdot 16\sigma\sqrt{\kappa n}\cdot\sqrt{n\log(n)}}\right) \\ \leq& \frac{q}{2\cdot 16\sigma\sqrt{\kappa n}\cdot\sqrt{n\log(n)}} \approx 0.3147. \end{aligned}$$

Dies führt, unabhängig von der Wahl des Approximationfaktors γ, nach Satz 4.19 zu keinem beweisbaren Vorteil, da der Hilfsparameter t zu klein ist. Die Wahl der Primzahl $q \approx 2^{35}$, führt dagegen zu einer beweisbaren Reduktion zum Mod-$\mathrm{GIVP}^{n_\epsilon}_{\gamma}$-Problem mit $\epsilon = n^{-\sqrt{\log(n)}}$ und $\gamma > 4\cdot 16\sigma\sqrt{\kappa n}\sqrt{n}\cdot\log(n)$. Somit ergibt sich durch die Reduktionskette(Abb. 6) eine Reduktion von Mod-$\mathrm{SIVP}_{\gamma'}$ zu der Binding-Eigenschaft, mit dem Approximationsfaktor:

$$\gamma' = \gamma\cdot\sqrt{\frac{\log(2n(1+n^{-\sqrt{\log(n)}}))}{\pi}} \approx 2^{37}.$$

Damit ist das Brechen der Binding-Eigenschaft mindestens so schwer wie das Lösen des SIVP-Problems, zu dem Approximationsfaktor γ' in einem 2^10-dimensionalen Modul-Gitter.

Da die Binding-Eigenschaft auf dem $\mathrm{SKS}^2_{R_q,16\sigma\sqrt{\kappa n},3}$-Problem basiert, lässt sich durch Satz 5.7 der Hermite-Faktor bestimmen, der benötigt wird, um die Binding-Sicherheit mit einem Gitterreduktionsverfahren zu brechen. Um die Hiding-Sicherheit abschätzen zu können, wird das zugehörige $\mathrm{DKS}_{m,\beta,h+l}$-Problem betrachtet. Mit Satz 5.6 lässt sich der Hermite-Faktor bestimmen, um einen gewissen Vorteil ϵ zu erhalten. Durch genügend häufige Wiederholung des Angriffs wird dieser Vorteil dementsprechend groß. Um die Anzahl der benötigten Taktzyklen abzuschätzen, die der BKZ-Algorithmus zu einem Hermite-Faktor δ_0 benötigt, verwenden wir die Schätzungen von Lindner und Peikert (4.1) sowie die Abschätzung von Albrecht (4.2).

Problem	**Hermite-Faktor**	**Taktzyklen - LAP**	**Taktzyklen - Albrecht**
Angriff - Binding	≈ 1.0024	$\approx 2^{738}$	$\approx 2^{435}$
Angriff - $\mathrm{DKS}_{m,\beta,h+l}$, $\epsilon = 1/100$	≈ 1.0032	$\approx 2^{424}$	$\approx 2^{310}$
Angriff - $\mathrm{SKS}^2_{R_q,16\sigma\sqrt{\kappa n},3}$	≈ 1.0035	$\approx 2^{365}$	$\approx 2^{282}$

Tabelle 6: Sicherheit von Binding, sowie Hiding

Der Angriff auf die Binding-Eigenschaft aus Kapitel 5.5.2 entspricht einem Angriff auf das $\mathrm{SKS}^2_{R_q,4\sigma\sqrt{n},3}$-Problem. In der letzten Zeile wird analog das $\mathrm{SKS}^2_{R_q,16\sigma\sqrt{\kappa n},3}$-Problem angegriffen, auf dem die Sicherheit der Binding-Eigenschaft beruht.

6 Fazit

Das Ziel dieser Arbeit war es, zu dem von Baum et. al. beschriebenen Commitment-Verfahren, Sicherheitsgarantien zu konkreten Parametern zu erhalten. Außerdem sollten detaillierte und vollständige Reduktionsbeweise zur Binding-Eigenschaft angegeben werden. In dieser Arbeit wurde, mithilfe bereits vorhandener Literatur, die Sicherheit des M-SIS-Problems im durchschnittlichen Fall auf die Sicherheit des Modul-SIVP-Problem im schwersten Fall zurückgeführt. Im Besonderen wurden Algorithmen angegeben, die nachweisbar, zu bestimmten Parametern eine Reduktion des Modul-SIVP-Problems zur Binding-Eigenschaft liefern. Dadurch ist es möglich, wie in Kapitel 5.6 beschrieben, die Sicherheit der Binding-Eigenschaft auf die Sicherheit des Modul-SIVP-Problems, zu einem genauen Approximationsfaktor γ zurückzuführen. Insbesondere basiert das Commitment-Verfahren, zu Parametern die wie in Satz 5.3 gewählt sind, auf der Sicherheit des Mod-SIVP$_\gamma$-Problems mit Approximationsfaktor

$$\gamma(N) = O\left(\beta(N)\sqrt{m(N)} \cdot (\log(N) \cdot N)^{3/2}\right).$$

Die Sicherheit der Hiding-Eigenschaft wurde auf die Schwierigkeit des DKS-Problem zurückgeführt, welche sich durch den Angriff aus Kapitel 5.5.1 abschätzen lässt. Diese Abschätzung ist jedoch mit Vorsicht zu genießen, da die Multiplikationsstruktur des Kreisteilungsrings nicht benutzt wird. Außerdem gibt es, wie in [15] beschrieben, weitere Angriffe auf LWE-Probleme mit kleinen Fehlern. Diese Angriffe könnten bessere Resultate liefern, als der in dieser Arbeit beschriebene Dual-Angriff.

Während für die Binding-Eigenschaft eine worst-to-average-case Reduktion angegeben wurde, fehlt diese Sicherheitsaussage für die Hiding-Eigenschaft. Wie von Langlois und Stehlé [4] beschrieben, kann das M-LWE Problem auf die Sicherheit des Mod-SIVP-Problems zurückführt werden. Um Sicherheitsgarantien zu einem bestimmten Approximationsfaktor bezüglich der Hiding-Eigenschaft zu erhalten, müsste wie in [4] das Mod-SIVP$_\gamma$ auf das DKS-Problem reduziert werden. Hierbei könnten Schwierigkeiten in der unterschiedlichen Fehler- und Geheimnis-Verteilung der Probleme auftreten.

Literatur

[1] C. Baum, I. Damgård, V. Lyubashevsky, S. Oechsner, and C. Peikert, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks* (D. Catalano and R. De Prisco, eds.), (Cham), pp. 368–385, Springer International Publishing, 2018.

[2] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: a cryptographic perspective*, vol. 671 of *The Kluwer International Series in Engineering and Computer Science*. Boston, Massachusetts: Kluwer Academic Publishers, Mar. 2002.

[3] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Advances in Cryptology – EUROCRYPT 2010* (H. Gilbert, ed.), (Berlin, Heidelberg), pp. 1–23, Springer Berlin Heidelberg, 2010.

[4] A. Langlois and D. Stehle, "Worst-case to average-case reductions for module lattices." Cryptology ePrint Archive, Report 2012/090, 2012. urlhttps://eprint.iacr.org/2012/090.

[5] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," vol. 60, pp. 1–23, 05 2010.

[6] C. Peikert, *A Decade of Lattice Cryptography* -. Singapore: Now Publishers, 2016.

[7] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on gaussian measures," vol. 37, pp. 372– 381, 11 2004.

[8] P. Reisert, "Post quantum security skript(vorläufig)," 2021.

[9] W. Ebeling and F. Hirzebruch, *Lattices and Codes: A Course Partially Based on Lectures by F. Hirzebruch*. Informatica International, Incorporated, 1994.

[10] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, Sept. 2009.

[11] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on gaussian measures," vol. 37, pp. 372– 381, 11 2004.

[12] C. Peikert, "Limits on the hardness of lattice problems in lp norms," *computational complexity*, vol. 17, pp. 300–351, 2007.

[13] C. Gentry, V. Vaikuntanathan, and C. Peikert, "How to use a short basis: Trapdoors for hard lattices and new cryptographic constructions," 2008.

[14] R. Lindner and C. Peikert, "Better key sizes (and attacks) for lwe-based encryption," in *Topics in Cryptology – CT-RSA 2011* (A. Kiayias, ed.), (Berlin, Heidelberg), pp. 319–339, Springer Berlin Heidelberg, 2011.

[15] R. Player, *Parameter selection in lattice-based cryptography.* PhD thesis, Royal Holloway, University of London, 2018.

[16] M. R. Albrecht, C. Cid, J.-C. Faugère, R. Fitzpatrick, and L. Perret, "On the complexity of the bkw algorithm on lwe." Cryptology ePrint Archive, Report 2012/636, 2012.

[17] D. Micciancio, "Almost perfect lattices, the covering radius problem, and applications to Ajtai's connection factor," *SIAM Journal on Computing*, vol. 34, no. 1, pp. 118–169, 2004. Preliminary version in STOC 2002.

[18] V. Lyubashevsky and G. Seiler, "Short, invertible elements in partially splitting cyclotomic rings and applications to lattice-based zero-knowledge proofs," in *Advances in Cryptology – EUROCRYPT 2018* (J. B. Nielsen and V. Rijmen, eds.), (Cham), pp. 204–224, Springer International Publishing, 2018.