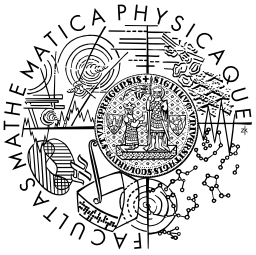

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Jan Václavek

Problém LWE a bezpečnost schémat pro výměnu klíče

Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Pavel Příhoda, Ph.D.

Studijní program: Matematika

Studijní obor: Obecná matematika

Praha 2019

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Rád bych poděkoval svému vedoucímu doc. Mgr. Pavlu Příhodovi, Ph.D. za odborné vedení, trpělivost a čas, který mi věnoval během zpracování bakalářské práce. Dále bych rád poděkoval své rodině a přítelkyni za péči a podporu během celého studia.

Název práce: Problém LWE a bezpečnost schémat pro výměnu klíče

Autor: Jan Václavek

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Pavel Příhoda, Ph.D., Katedra algebry

Abstrakt: Hrozba silného kvantového počítače vede ke snaze založit kryptosystémy na problémech, které budou těžké i pro kvantový počítač. V této práci si představíme problém LWE, o kterém se předpokládá, že by takovým problémem mohl být. Nejprve si představíme mříže, které s problémem LWE úzce souvisí. Zavedeme základní pojmy, popíšeme mřížové problémy a vyřešíme cvičení týkající se pokrývajícího poloměru mříže. Poté definujeme problém LWE, představíme jeho varianty a ukážeme redukce dvou mřížových problémů na vhodnou variantu problému LWE. K tomuto účelu definujeme pojem statistické vzdálenosti a dokážeme o něm tvrzení, která potřebujeme pro redukci. Nakonec ukážeme konkrétní využití problému LWE. Popíšeme schéma na výměnu klíče a naznačíme, jak dokázat jeho bezpečnost za předpokladu, že problém LWE je těžký.

Klíčová slova: LWE problém, mříž, výměna klíče

Title: LWE and provably secure key exchange schemes

Author: Jan Václavek

Department: Department of Algebra

Supervisor: doc. Mgr. Pavel Příhoda, Ph.D., Department of Algebra

Abstract: The threat of large-scale quantum computers motivates cryptographers to base cryptosystems on problems believed to be resistant against quantum computers. In this thesis, we focus on the LWE problem which is believed to be resistant against quantum computers. First, we describe lattices which are closely related to the LWE problem. We introduce basic notions, describe lattice problems and solve exercises related to the covering radius of lattice. After that, we introduce the LWE problem and its variants. We prove reductions from two lattice problems to certain variant of the LWE problem. We define the notion of statistical distance and prove some lemmata about it which we need within reductions. Moreover, we show concrete application of the LWE problem. We describe a scheme for key exchange and briefly prove its security under the assumption that the LWE problem is hard.

Keywords: LWE problem, lattice, key exchange

Obsah

Úvod

Mnoho dnešních kryptosystémů, jako je například RSA nebo Diffie-Hellmanův protokol, je založeno na těžkých problémech z teorie čísel. V roce 1997 byl ovšem popsán kvantový algoritmus, který tyto problémy, mezi něž patří například faktorizace celých čísel a diskrétní logaritmus, řeší v polynomiálním čase. To v kombinaci s možností, že se reálně povede postavit silný kvantový počítač, vede ke snaze založit kryptosystémy na problémech, které budou těžké i pro kvantový počítač.

Věří se, že jedním z takových problémů by mohl být problém LWE (*Learning with Errors*). Ten poprvé popsal v roce 2005 Oded Regev [1]. Neformálně se jedná o řešení soustavy polynomiálně mnoha lineárních rovnic modulo p, kde je pravá strana soustavy pozměněna chybou z předem známé chybové distribuce.

Regev ve své práci mimo jiné ukázal, že se jistý mřížový problém, nazývaný nejkratší vektor mříže, kvantově redukuje na problém LWE. To znamená, že pokud bychom byli schopni řešit problém LWE, uměli bychom kvantově řešit tento mřížový problém. Později byla popsána i nekvantová redukce pro speciální verzi problému nejkratšího vektoru mříže [2]. Zmíněné redukce patří mezi hlavní důvody, proč se věří, že problém LWE je těžký. I přes velké úsilí se totiž zatím nepovedlo najít efektivní algoritmus, který by, klasicky nebo kvantově, řešil zmíněné mřížové problémy.

V této práci se nejprve podíváme na mříže. Definujeme základní pojmy, uvedeme vztahy mezi nimi a popíšeme základní mřížové problémy. Kromě toho vyřešíme také cvičení ukazující existenci mříží, které splňují zajímavé podmínky a jejichž explicitní popis přitom nemusí být zřejmý.

V další části se zaměříme na problém LWE a jeho varianty. Ukážeme, jak fungují redukce mřížových problémů na problém LWE. Především se podíváme na nekvantovou část redukce z článku [1], kde mřížovým problémem je problém nejbližšího vektoru, a na její rozšíření z článku [2], kde mřížovým problémem je speciální verze problému nejkratšího vektoru. K tomu si zavedeme pojmy jako je například Gaussovo rozdělení na mříži nebo statistická vzdálenost a ukážeme si, jak je v takových redukcích využít.

Nakonec ukážeme konkrétní využití problému LWE. Ve stručnosti popíšeme schéma na výměnu klíče, jehož bezpečnost je založena právě na problému LWE.

1. Značení a definice

- Matice budeme značit velkými tučnými písmeny, vektory malými tučnými písmeny. Výrazem $\mathbf{b}_i$ budeme značit i-tý sloupcový vektor matice $\mathbf{B}$. Vektory budeme chápat jako sloupcové a i-tou složku vektoru $\mathbf{a}$ budeme označovat a_i. Matici $\mathbf{B}$ budeme ztotožňovat s posloupností jejích sloupcových vektorů $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$.
- Pro vektor $\mathbf{x} \in \mathbb{R}^n$ budeme značit výrazem $\|\mathbf{x}\|$ jeho délku, definovanou jako
$$\|\mathbf{x}\| = \sqrt{\sum_{i=1}^{n} x_i^2}.$$
- Buď $A \subset \mathbb{R}^n$ a $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. Potom definujeme $\operatorname{dist}(\mathbf{x}, \mathbf{y})$ jako
$$\operatorname{dist}(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|$$
a výrazem $\operatorname{dist}(A, \mathbf{x})$ budeme rozumět
$$\operatorname{dist}(A, \mathbf{x}) = \inf_{\mathbf{a} \in A} \|\mathbf{a} - \mathbf{x}\|.$$
- Skalární součin dvou vektorů $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ definujeme jako
$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^\top \mathbf{y} = \sum_{i=1}^{n} x_i y_i.$$
- Pro $A \subset \mathbb{R}^n$ Lebesgueovsky měřitelnou budeme výrazem $\operatorname{vol}(A)$ značit n-rozměrný objem množiny A.
- Pro množinu $A \subset \mathbb{R}^n$ definujeme výrazem $\operatorname{span}(A)$ lineární obal A definovaný jako
$$\operatorname{span}(A) = \left\{ \sum_{i=1}^{k} x_i \mathbf{a}_i : x_i \in \mathbb{R},\, \mathbf{a}_i \in A,\, k \in \mathbb{N} \right\}.$$
- Výrazem $(a \pm b) \cdot c$, kde a, b, c jsou reálná, budeme označovat otevřený interval $((a - b) \cdot c, (a + b) \cdot c)$.
- Otevřenou jednotkovou kouli v $\mathbb{R}^n$ se středem v počátku budeme značit $\mathcal{B}_n$.
- Výrazem $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ budeme značit aditivní grupu na reálném intervalu [0,1) se sčítáním modulo 1.
- Pravděpodobnostním algoritmem budeme rozumět algoritmus, který během výpočtu činí náhodné volby.
- Efektivním algoritmem budeme rozumět algoritmus pracující v polynomiálním čase.
- Výrazem $\lfloor x \rceil$, kde $x \in \mathbb{R}$, budeme značit nejbližší celé číslo k x. V případě, kdy taková čísla existují dvě, volíme větší z obou možných čísel.

- Výrazem poly(n) budeme značit reálnou polynomiální funkci celočíselné proměnné.

Definice 1. *Mějme funkce* $f : \mathbb{N} \to \mathbb{R}^+$, $g : \mathbb{N} \to \mathbb{R}^+$ *a* $p : \mathbb{N} \to [0,1]$. *Potom definujeme jejich asymptotické chování následujícím způsobem:*

- $f(n) = \Omega(g(n)) \iff \exists c > 0 \ \exists n_0 \ \forall n > n_0 : f(n) \geq c \cdot g(n)$,
- $f(n) = \omega(g(n)) \iff \forall c > 0 \ \exists n_0 \ \forall n > n_0 : f(n) \geq c \cdot g(n)$,
- *řekneme, že* $f(n)$ *je zanedbatelnou funkcí, značíme* $f(n) = \text{negl}(n)$, *pokud* $\forall c > 0 \ \exists n_0 \ \forall n > n_0 : f(n) < n^{-c}$,
- *řekneme, že pravděpodobnost* $p(n)$ *je velká, pokud* $p(n) = 1 - \text{negl}(n)$.

2. Mříže

V této kapitole budeme vycházet především z knihy [3] a z poznámek [4, 5].

2.1 Základní pojmy

Definice 2 (Mříž)**.** *Nechť* $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\} \subset \mathbb{R}^n$ *je posloupnost* m *lineárně nezávislých vektorů.* Mříž Λ *generovanou těmito vektory definujeme jako*

$$\Lambda = \mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^{m} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\}.$$

Vektory $\mathbf{b}_1, \ldots, \mathbf{b}_m$ *nazýváme* bází *mříže.* Dimenzí *mříže rozumíme hodnotu* n *a* hodností *mříže rozumíme hodnotu* m*.*

Ekvivalentně se jedná o diskrétní aditivní podgrupu $\mathbb{R}^n$. To je důvod, proč jsme požadovali, aby vektory v definici byly lineárně nezávislé. Například množina $\Lambda \subset \mathbb{R}$ generovaná dvojicí vektorů $\mathbf{b}_1 = 1, \mathbf{b}_2 = \pi$ není diskrétní, protože existuje nenulový vektor $\mathbf{v} \in \Lambda$ s libovolně malou kladnou normou. Pokud budeme uvažovat posloupnost $\mathbf{B}$ jako matici $n \times m$ se sloupci $\mathbf{b}_1, \ldots, \mathbf{b}_m$, můžeme mříž s bází $\mathbf{B}$ definovat ekvivalentně jako

$$\mathcal{L}(\mathbf{B}) = \mathbf{B}\mathbb{Z}^m = \{\mathbf{B}\mathbf{x} : \mathbf{x} \in \mathbb{Z}^m\}.$$

Až na definici 8 a první půlku důkazu cvičení 1 budeme uvažovat mříže, kde $m = n$. Proto výrazem báze můžeme uvažovat jak bázi prostoru $\mathbb{R}^n$, tak příslušné mříže. Každá mříž má nekonečně mnoho bází. Například matice $\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ a $\mathbf{B} = \begin{pmatrix} 2100 & 1027 \\ 1963 & 960 \end{pmatrix}$ generují stejnou mříž, konkrétně $\mathbb{Z}^2$, což nemusí být na první pohled zřejmé. Jak poznat, kdy dvě matice určují stejnou mříž, shrnuje následující lemma.

Lemma 1 ([4, Theorem 3])**.** *Matice* $\mathbf{A}$ *a* $\mathbf{B}$ *určují stejnou mříž právě tehdy, když existuje matice* $\mathbf{C}$ *s celočíselnými prvky a determinantem* ± 1 *taková, že* $\mathbf{A} = \mathbf{B}\mathbf{C}$*.*

Definice 3 (Determinant)**.** *Buď* Λ *mříž s bází* $\mathbf{B}$*.* Determinant *mříže* Λ *definujeme jako*

$$\det(\Lambda) = |\det(\mathbf{B})|.$$

Definice je korektní, tedy nezávisí na bázi mříže, kvůli předchozímu lemmatu a multiplikativitě determinantu.

Definice 4 (Duální mříž)**.** *Buď* Λ *n-dimenzionální mříž.* Duální mříž *k* Λ*, označovanou* Λ^**, definujeme jako*

$$\Lambda^* = \left\{ \mathbf{x} \in \mathbb{R}^n : (\forall \mathbf{v} \in \Lambda)\, (\langle \mathbf{x}, \mathbf{v} \rangle \in \mathbb{Z}) \right\}.$$

Z linearity skalárního součinu a definice mříže stačí podmínku z předchozí definice ověřovat pouze na vektorech libovolné báze mříže Λ. Z toho plyne, že pokud je $\mathbf{B}$ báze mříže Λ, potom je $\left(\mathbf{B}^{-1}\right)^{\top}$, což budeme dále značit $\mathbf{B}^{*}$, bází duální mříže Λ^{*}. Platí tedy, že $(\Lambda^{*})^{*} = \Lambda$.

Pro uspořádanou množinu $\mathbf{S} = \{\mathbf{s}_1, \ldots, \mathbf{s}_m\} \subset \mathbb{R}^n$ m lineárně nezávislých vektorů označujeme jako $\widetilde{\mathbf{S}} = \{\widetilde{\mathbf{s}}_1, \ldots, \widetilde{\mathbf{s}}_m\}$ Gramovu-Schmidtovu ortogonalizaci posloupnosti $\mathbf{S}$. Tu definujeme iterativně jako $\widetilde{\mathbf{s}}_1 = \mathbf{s}_1$ a pro $i = 2, \ldots, m$ jako

$$\widetilde{\mathbf{s}}_i = \mathbf{s}_i - \sum_{j=1}^{i-1} \frac{\langle \mathbf{s}_i, \widetilde{\mathbf{s}}_j \rangle}{\langle \widetilde{\mathbf{s}}_j, \widetilde{\mathbf{s}}_j \rangle} \widetilde{\mathbf{s}}_j.$$

V souvislosti s duálními mřížemi je někdy výhodné ortogonalizovat v opačném pořadí, kdy definujeme $\widetilde{\mathbf{s}}_m = \mathbf{s}_m$ a pro $i = m-1, \ldots, 1$

$$\widetilde{\mathbf{s}}_i = \mathbf{s}_i - \sum_{j=i+1}^{m} \frac{\langle \mathbf{s}_i, \widetilde{\mathbf{s}}_j \rangle}{\langle \widetilde{\mathbf{s}}_j, \widetilde{\mathbf{s}}_j \rangle} \widetilde{\mathbf{s}}_j.$$

Další parametr mříže, nazývaný minimální vzdálenost, hraje důležitou roli v redukcích.

Definice 5 (Minimální vzdálenost)**.** Minimální vzdálenost $\lambda_1(\Lambda)$ *mříže* Λ *definujeme jako minimální vzdálenost mezi dvěma libovolnými různými vektory mříže:*

$$\lambda_1(\Lambda) = \min_{x \neq y \in \Lambda} \|x - y\|.$$

V definici jsme použili minimum místo infima, protože mříž je diskrétní množinou a infima se nabývá. Ekvivalentně se jedná o velikost nejkratšího nenulového vektoru mříže. Bude se nám hodit následující jednoduchý dolní odhad na minimální vzdálenost.

Lemma 2 ([3, Theorem 1.1])**.** *Pro každou bázi* $\mathbf{B}$ *a její Gramovu-Schmidtovu ortogonalizaci* $\widetilde{\mathbf{B}}$ *platí, že* $\lambda_1(\mathcal{L}(\mathbf{B})) \geq \min_i \|\widetilde{\mathbf{b}}_i\|$.

Následující lemma nám shrnuje vztah mezi Gramovou-Schmidtovou ortogonalizací a dualitou mříží.

Lemma 3 ([2, Lemma 2.2])**.** *Nechť* $\mathbf{B}$ *je báze a* $\mathbf{D} = \mathbf{B}^{*}$ *její duální báze. Potom platí* $\widetilde{\mathbf{d}}_i = \widetilde{\mathbf{b}}_i / \|\widetilde{\mathbf{b}}_i\|^2$ *pro každé* $i = 1, \ldots, n$*, kde báze* $\mathbf{D}$ *je ortogonalizována v opačném pořadí. Speciálně platí* $\|\widetilde{\mathbf{d}}_i\| = 1/\|\widetilde{\mathbf{b}}_i\|$.

Uvažujme nyní bázi $\mathbf{B}$ a příslušnou mříž $\Lambda = \mathcal{L}(\mathbf{B})$. Platí, že

$$\lambda_1(\Lambda) \leq \min_i \|\mathbf{b}_i\|,$$

protože každý sloupec matice $\mathbf{B}$ je nenulový vektor mříže. V další části ukážeme lepší odhad, který navíc nezávisí na volbě báze $\mathbf{B}$. Mříž s libovolně velkou minimální vzdáleností existuje, protože pro $c > 0$ platí $\lambda_1(c \cdot \Lambda) = c \cdot \lambda_1(\Lambda)$. Zajímá nás, jestli existuje mříž s libovolně velkou minimální vzdáleností i v případě, kdy máme předepsanou hodnotu determinantu. Jinými slovy, pokud jsme schopni odhadnout podíl

$$\frac{\lambda_1(\Lambda)}{\det(\Lambda)^{\frac{1}{n}}}.$$

Z historických důvodů matematici zkoumali druhou mocninu této veličiny, která se nazývá Hermitův faktor.

Definice 6 (Hermitův faktor a konstanta)**.** Hermitův faktor *n-dimenzionální mříže* Λ *definujeme jako*

$$\gamma(\Lambda) = \left(\frac{\lambda_1(\Lambda)}{\det(\Lambda)^{\frac{1}{n}}} \right)^2 .$$

Hermitovu konstantu γ_n *v dimenzi* n *definujeme jako supremum přes všechny* n*-dimenzionální mříže, tedy* $\gamma_n = \sup_\Lambda \gamma(\Lambda)$*.*

Horní odhad provedeme pomocí tvrzení Minkowského.

Tvrzení 4 ([3, Theorem 1.4])**.** *Mějme* n*-dimenzionální mříž* Λ*. Pokud* $S \subset \mathbb{R}^n$ *je symetrická konvexní taková, že* $\mathrm{vol}(S) > 2^n \det(\Lambda)$*, potom* S *obsahuje nenulový vektor mříže* Λ*.*

Předchozí tvrzení použijeme na horní odhad minimální vzdálenosti mříže Λ.

Důsledek 5. *Pro Hermitovu konstantu platí* $\gamma_n \leq n$*. Jinými slovy, pro každou* n*-dimenzionální mříž* Λ *existuje vektor* $\mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}$ *splňující*

$$\|\mathbf{x}\| \leq \sqrt{n} \det(\Lambda)^{\frac{1}{n}} .$$

Důkaz. Pro spor předpokládejme, že pro nějakou mříž Λ platí

$$\lambda_1(\Lambda) > \sqrt{n} \det(\Lambda)^{\frac{1}{n}}$$

a označme $l = \lambda_1(\Lambda)$. Uvažujme otevřenou hyperkrychli C o délce hrany $\frac{2l}{\sqrt{n}}$ se středem v počátku. Potom z předpokladu platí

$$\mathrm{vol}(C) = \frac{(2l)^n}{n^{\frac{n}{2}}} > 2^n \det(\Lambda) .$$

Použitím předchozího tvrzení dostaneme vektor $\mathbf{x} \in C \cap \Lambda$. Z volby C platí $\|\mathbf{x}\| < \sqrt{\frac{l^2}{n} + \cdots + \frac{l^2}{n}} = l = \lambda_1(\Lambda)$, což je spor. □

Minimální vzdálenost mříže Λ jsme mohli ekvivalentně definovat jako nejmenší $r > 0$ takové, že uzavřená koule o poloměru r se středem v počátku obsahuje nenulový vektor mříže. Tuto definici můžeme zobecnit.

Definice 7 (Postupné minimum)**.** *Pro* n*-dimenzionální mříž* Λ *a celé* $k \leq n$ *definujeme* k-té postupné minimum $\lambda_k(\Lambda)$ *jako nejmenší* $r > 0$ *takové, že uzavřená koule o poloměru* r *se středem v počátku obsahuje* k *lineárně nezávislých vektorů mříže* Λ*.*

Podobně jako jsme ukázali horní odhad pro $\lambda_1(\Lambda)$, existuje horní odhad pro geometrický průměr všech postupných minim.

Tvrzení 6 ([3, Theorem 1.5])**.** *Nechť* Λ *je* n*-dimenzionální mříž. Potom*

$$\left(\prod_{i=1}^{n} \lambda_i(\Lambda) \right)^{1/n} \leq \sqrt{n} \cdot \det(\Lambda)^{1/n} .$$

Definice 8 (Základní rovnoběžnostěn, Centrovaný základní rovnoběžnostěn, Základní oblast)**.** *Mějme posloupnost* $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\} \subset \mathbb{R}^n$ *m lineárně nezávislých vektorů.* Základní rovnoběžnostěn *odpovídající posloupnosti* $\mathbf{B}$ *definujeme jako množinu bodů*

$$\mathcal{P}(\mathbf{B}) = \left\{ \sum_{i=1}^{m} x_i \mathbf{b}_i : 0 \leq x_i < 1 \right\}.$$

Centrovaný základní rovnoběžnostěn *odpovídající posloupnosti* $\mathbf{B}$ *definujeme jako množinu bodů*

$$\mathcal{P}_{1/2}(\mathbf{B}) = \left\{ \sum_{i=1}^{m} x_i \mathbf{b}_i : -\frac{1}{2} \leq x_i < \frac{1}{2} \right\}.$$

Množinu $\mathcal{R} \subset \operatorname{span}(\Lambda)$*, kde* Λ *je n-dimenzionální mříž hodnosti m, nazveme* základní oblastí *mříže* Λ*, pokud množiny* $\mathbf{v} + \mathcal{R}$*, kde* $\mathbf{v} \in \Lambda$*, tvoří disjunktní pokrytí* $\operatorname{span}(\Lambda)$*.*

Pro bod $\mathbf{w} \in \mathbb{R}^n$ a bázi $\mathbf{B}$ označujeme výrazem $\mathbf{x} = \mathbf{w} \bmod \mathbf{B}$ jednoznačně určený vektor $\mathbf{x} \in \mathcal{P}_{1/2}(\mathbf{B})$ takový, že $\mathbf{w} - \mathbf{x} \in \mathcal{L}(\mathbf{B})$. Na vstupu s bází $\mathbf{B}$ a vektorem $\mathbf{w} \in \mathbb{R}^n$ spočítáme takové $\mathbf{x}$ snadno jako $\mathbf{x} = \mathbf{w} - \mathbf{B}\lfloor \mathbf{B}^{-1}\mathbf{w} \rceil$. Různé báze mříže obecně definují různé rovnoběžnostěny, ale všechny mají stejný n-rozměrný objem. Obě množiny $\mathcal{P}(\mathbf{B})$ a $\mathcal{P}_{1/2}(\mathbf{B})$ tvoří základní oblast mříže $\Lambda = \mathcal{L}(\mathbf{B})$.

2.2 Pokrývající poloměr

V této části se podrobněji podíváme na další parametr mříže nazývaný pokrývající poloměr a vyřešíme cvičení, která se ho týkají. Budeme vycházet z [5], odkud jsou převzata i cvičení.

Definice 9 (Pokrývající poloměr)**.** *Buď* Λ *n-dimenzionální mříž.* Pokrývající poloměr $\mu(\Lambda)$ *mříže* Λ *definujeme jako nejmenší* $\mu > 0$ *takové, že uzavřené koule* $\mathbf{v} + \mu \cdot \overline{\mathcal{B}}_n$*, kde* $\mathbf{v} \in \Lambda$*, pokrývají celé* $\mathbb{R}^n$*.*

Následující lemma nám dává dolní odhad na pokrývající poloměr.

Lemma 7 ([5, Lemma 18])**.** *Pro každou n-dimenzionální mříž* Λ *platí, že pokrývající poloměr* $\mu(\Lambda) \geq \frac{1}{2}\lambda_n(\Lambda)$*.*

Horní odhad odvodíme v následujícím cvičení.

Cvičení 1. *Ukažte, že pro každou n-dimenzionální mříž* Λ *platí*

$$\mu(\Lambda) \leq \frac{\sqrt{n}}{2}\lambda_n(\Lambda).$$

Důkaz. Abychom mohli použít matematickou indukci, potřebujeme uvažovat také mříže s menší hodností. První část tohoto důkazu je spolu s definicemi 2 a 8 jediným místem, kde mříže menší hodnosti uvažujeme.

Nejprve ukážeme, že $\mathcal{P}(\widetilde{\mathbf{B}}) + \mathbf{w}$, kde $\mathbf{w} \in \operatorname{span}(\widetilde{\mathbf{B}})$ je libovolné, tvoří základní oblast n-dimenzionální mříže $\mathcal{L}(\mathbf{B})$ hodnosti m pro libovolnou posloupnost $\mathbf{B}$ m lineárně nezávislých vektorů. K tomu nám stačí ukázat, že $\mathcal{P}(\widetilde{\mathbf{B}})$ tvoří základní oblast, protože posunutí zachovává pokrytí i disjunktnost. Postupujme tedy indukcí podle hodnosti mříže m. Pro $m = 1$ to platí, protože v takovém případě

$\mathcal{P}(\widetilde{\mathbf{B}}) = \mathcal{P}(\mathbf{B})$. Dále označme $\Lambda' = \mathcal{L}(\{\mathbf{b}_1, \ldots, \mathbf{b}_{m-1}\})$. Mříž $\mathcal{L}(\mathbf{B})$ si můžeme „rozložit na vrstvy“, platí totiž

$$\mathcal{L}(\mathbf{B}) = \bigcup_{c \in \mathbb{Z}} \Lambda' + c \cdot \mathbf{b}_m.$$

Z indukčního předpokladu tvoří množiny $\mathbf{w} + \mathcal{P}(\{\widetilde{\mathbf{b}}_1, \ldots, \widetilde{\mathbf{b}}_{m-1}\})$, kde $\mathbf{w} \in \Lambda'$, disjunktní pokrytí $\operatorname{span}(\Lambda')$. Tedy také množiny $\mathbf{w} + \mathcal{P}(\{\widetilde{\mathbf{b}}_1, \ldots, \widetilde{\mathbf{b}}_{m-1}\})$, kde $\mathbf{w} \in \Lambda' + c \cdot \mathbf{b}_m$, tvoří disjunktní pokrytí prostoru $\operatorname{span}(\Lambda') + c \cdot \mathbf{b}_m$. Z vlastností Gramovy-Schmidtovy ortogonalizace pro každé $c \in \mathbb{Z}$ platí

$$\operatorname{span}(\Lambda') + c \cdot \mathbf{b}_m + \widetilde{\mathbf{b}}_m = \operatorname{span}(\Lambda') + (c+1) \cdot \mathbf{b}_m.$$

Dohromady tedy dostaneme, že množiny $\mathbf{v} + \mathcal{P}(\{\widetilde{\mathbf{b}}_1, \ldots, \widetilde{\mathbf{b}}_m\})$, kde $\mathbf{v} \in \Lambda$, tvoří disjunktní pokrytí $\operatorname{span}(\Lambda)$. Tím jsme ukázali, že $\mathcal{P}(\widetilde{\mathbf{B}})$ tvoří základní oblast n-dimenzionální mříže $\mathcal{L}(\mathbf{B})$. Přistoupíme k samotnému důkazu cvičení.

Nechť $\mathbf{V} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subset \Lambda$ jsou lineárně nezávislé vektory délky nejvýše $\lambda_n(\Lambda)$, které existují z definice n-tého postupného minima. Platí $\mathcal{L}(\mathbf{V}) \subset \Lambda$, a tedy $\mu(\Lambda) \leq \mu(\mathcal{L}(\mathbf{V}))$. Nyní odhadneme $\mu(\mathcal{L}(\mathbf{V}))$. K tomu využijeme, že množina $\mathcal{P}(\widetilde{\mathbf{V}}) - \frac{1}{2}(\widetilde{\mathbf{v}}_1 + \cdots + \widetilde{\mathbf{v}}_n) = \mathcal{P}_{1/2}(\widetilde{\mathbf{V}})$ tvoří základní oblast mříže $\mathcal{L}(\mathbf{V})$. Označme $\widetilde{\mathbf{W}}$ matici s i-tým sloupcem $\lambda_n(\Lambda) \cdot \widetilde{\mathbf{v}}_i / \|\widetilde{\mathbf{v}}_i\|$. Protože pro každé i platí $\|\widetilde{\mathbf{v}}_i\| \leq \|\mathbf{v}_i\| \leq \lambda_n(\Lambda)$, dostaneme, že

$$\mathcal{P}(\widetilde{\mathbf{V}}) \subset \mathcal{P}(\widetilde{\mathbf{W}}),$$

a tedy

$$\mathcal{P}(\widetilde{\mathbf{V}}) - \frac{1}{2}(\widetilde{\mathbf{v}}_1 + \cdots + \widetilde{\mathbf{v}}_n) \subset \mathcal{P}(\widetilde{\mathbf{W}}) - \frac{1}{2}(\widetilde{\mathbf{w}}_1 + \cdots + \widetilde{\mathbf{w}}_n).$$

Pro každý $\mathbf{x} \in \mathcal{P}(\widetilde{\mathbf{W}}) - \frac{1}{2}(\widetilde{\mathbf{w}}_1 + \cdots + \widetilde{\mathbf{w}}_n) = \mathcal{P}_{1/2}(\widetilde{\mathbf{W}})$ platí

$$\|\mathbf{x}\| \leq \frac{\sqrt{\lambda_n(\Lambda)^2 + \cdots + \lambda_n(\Lambda)^2}}{2} = \frac{\sqrt{n}}{2} \lambda_n(\Lambda),$$

a tedy

$$\mathcal{P}(\widetilde{\mathbf{V}}) - \frac{1}{2}(\widetilde{\mathbf{v}}_1 + \cdots + \widetilde{\mathbf{v}}_n) \subset \frac{\sqrt{n}}{2} \lambda_n(\Lambda) \cdot \overline{\mathcal{B}}_n.$$

Protože $\mathcal{P}(\widetilde{\mathbf{V}}) - \frac{1}{2}(\widetilde{\mathbf{v}}_1 + \cdots + \widetilde{\mathbf{v}}_n)$ tvoří základní oblast, jsme hotovi. □

Pro každé n existuje mříž Λ taková, že $\mu(\Lambda) = \frac{\sqrt{n}}{2} \lambda_n(\Lambda)$. Jako nejjednodušší příklad uvedeme mříž $\Lambda = \mathbb{Z}^n$.

Obecněji, pro každé $n \in \mathbb{N}$ a $\frac{1}{2} < c \leq \frac{\sqrt{n}}{2}$ existuje n-dimenzionální mříž Λ taková, že $\mu(\Lambda) = c\lambda_n(\Lambda)$. Jako příklad uvedeme mříž $\Lambda = \mathcal{L}(\mathbf{B})$, kde

$$\mathbf{B} = \begin{pmatrix} a & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}, \quad a = \sqrt{\frac{n-1}{4c^2 - 1}}.$$

Víme, že pro každou n-dimenzionální mříž Λ platí nerovnosti

$$\lambda_1(\Lambda) \leq \lambda_2(\Lambda) \leq \cdots \leq \lambda_n(\Lambda) \leq 2\mu(\Lambda) \leq \sqrt{n} \lambda_n(\Lambda).$$

Pomocí dalších cvičení ukážeme, že existují mříže, kde $\mu(\Lambda)$ je blízko $\lambda_1(\Lambda)$.

Cvičení 2. *Buď Λ n-dimenzionální mříž a buď $\mathbf{v} \in \Lambda$. Dokažte, že $\Lambda' = \Lambda \cup (\Lambda + \frac{\mathbf{v}}{2})$ je také mříž. Navíc pokud $\frac{\mathbf{v}}{2}$ je ve vzdálenosti alespoň $\lambda_1(\Lambda)$ od mříže Λ, potom platí $\lambda_1(\Lambda') = \lambda_1(\Lambda)$ a $\det(\Lambda') = \det(\Lambda)/2$.*

Důkaz. Využijeme zmíněnou ekvivalentní definici mříže, která říká, že mříž je diskrétní aditivní podgrupa $\mathbb{R}^n$. Nejprve ukážeme, že Λ' je aditivní podgrupou $\mathbb{R}^n$.

- $\mathbf{0} \in \Lambda'$, protože $\mathbf{0} \in \Lambda$.
- uzavřenost na inverzní prvky: Buď $\mathbf{a} \in \Lambda'$. Potom buď $\mathbf{a} \in \Lambda$ a jsme hotovi, nebo $\mathbf{a} = \mathbf{w} + \frac{\mathbf{v}}{2}$ pro $\mathbf{w} \in \Lambda$. Potom $-\mathbf{a} = -\mathbf{w} - \frac{\mathbf{v}}{2} = (-\mathbf{w} - \mathbf{v}) + \frac{\mathbf{v}}{2}$.
- uzavřenost na sčítání: Nechť $\mathbf{a}, \mathbf{b} \in \Lambda'$. Rozlišíme tři případy. Pokud $\mathbf{a}$ i $\mathbf{b} \in \Lambda$, jsme hotovi. Pokud $\mathbf{a} \in \Lambda$ a $\mathbf{b} = \mathbf{w} + \frac{\mathbf{v}}{2}$ pro $\mathbf{w} \in \Lambda$, máme $\mathbf{a}+\mathbf{b} = (\mathbf{a}+\mathbf{w}) + \frac{\mathbf{v}}{2} \in \Lambda'$. Nakonec pokud $\mathbf{a} = \mathbf{u} + \frac{\mathbf{v}}{2}, \mathbf{b} = \mathbf{w} + \frac{\mathbf{v}}{2}$ pro $\mathbf{u}, \mathbf{w} \in \Lambda$, potom $\mathbf{a} + \mathbf{b} = \mathbf{u} + \mathbf{v} + \mathbf{w} \in \Lambda \subset \Lambda'$.

Λ' je diskrétní, protože Λ i $\Lambda + \frac{\mathbf{v}}{2}$ jsou diskrétní a konečné sjednocení zachovává tuto vlastnost.

Dále předpokládejme, že $\frac{\mathbf{v}}{2}$ je ve vzdálenosti alespoň $\lambda_1(\Lambda)$ od mříže Λ. Je zřejmé, že $\lambda_1(\Lambda') \leq \lambda_1(\Lambda)$. Ukážeme, že platí i druhá nerovnost. Pro spor předpokládejme, že ne, a tedy že $\lambda_1(\Lambda') < \lambda_1(\Lambda)$. Tedy existuje $\mathbf{w} \in \Lambda$ takový, že $\|\mathbf{w} + \frac{\mathbf{v}}{2}\| < \lambda_1(\Lambda)$. Podíváme-li se na vzdálenost $\frac{\mathbf{v}}{2}$ od $-\mathbf{w} \in \Lambda$, dostaneme spor. Tedy $\lambda_1(\Lambda') = \lambda_1(\Lambda)$.

Ukážeme, že poslední část s determinantem platí pro každý vektor $\mathbf{v} \in \Lambda$ takový, že $\frac{\mathbf{v}}{2} \notin \Lambda$, což vektor ze zadání splňuje, protože jinak by jeho vzdálenost od mříže Λ byla nula. Buď $\mathbf{B}$ libovolná báze mříže Λ. Označme $\mathbf{k} \in \mathbb{Z}^n$ souřadnice vektoru $\mathbf{v}$ vůči bázi $\mathbf{B}$. Každou souřadnici si rozložíme jako $k_i/2 = a_i + \frac{1}{2}a'_i$, kde $a_i \in \mathbb{Z}, a'_i \in \{0,1\}$. Protože $\frac{\mathbf{v}}{2} \notin \Lambda$, je alespoň jedno a'_i nenulové. Protože je mříž aditivní grupa, platí $\Lambda + \frac{\mathbf{v}}{2} = \Lambda + \frac{\mathbf{v}}{2} + \mathbf{w}$ pro $\mathbf{w} \in \Lambda$. V našem případě zvolme $\mathbf{w} = -a_1\mathbf{b}_1 - \ldots - a_n\mathbf{b}_n$. Označme $\frac{\mathbf{v}'}{2} = \frac{\mathbf{v}}{2} + \mathbf{w} = \frac{1}{2}a'_1\mathbf{b}_1 + \cdots + \frac{1}{2}a'_n\mathbf{b}_n$, tedy $\mathbf{v}' = a'_1\mathbf{b}_1 + \cdots + a'_n\mathbf{b}_n$. Tvrzení tedy můžeme bez újmy na obecnosti dokazovat pro $\mathbf{v}$ tvaru $\mathbf{v} = \mathbf{b}_{i_1} + \cdots + \mathbf{b}_{i_k}$, kde $1 \leq i_1 < \cdots < i_k \leq n$. Připomeneme, že pokud je $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ báze mříže Λ, potom je $\{\mathbf{b}_1 + \mathbf{b}_2, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ také báze stejné mříže. Opakováním předchozí poznámky dostaneme, že existuje báze mříže Λ obsahující naše $\mathbf{v}$. Vezmeme-li tuto bázi a nahradíme-li náš vektor $\mathbf{v}$ vektorem $\frac{\mathbf{v}}{2}$, dostaneme bázi mříže Λ'. Odtud a z linearity determinantu plyne tvrzení. □

Cvičení 3. *Buď Λ libovolná n-dimenzionální mříž. Potom existuje $\mathbf{h} \in \mathbb{R}^n$, jehož vzdálenost od mříže Λ je právě $\mu(\Lambda)$.*

Důkaz. Platí $\mu(\Lambda) = \sup_{\mathbf{x} \in \mathbb{R}^n} \operatorname{dist}(\mathbf{x}, \Lambda)$. Ukážeme, že se tohoto suprema nabývá. Z definice suprema zvolme pro každé $i \in \mathbb{N}$ bod $\mathbf{x}'_i \in \mathbb{R}^n$ takový, že

$$\operatorname{dist}(\mathbf{x}'_i, \Lambda) > \mu(\Lambda) - 2^{-i}.$$

Buď $\mathbf{v}_i \in \Lambda$ vektor splňující $\operatorname{dist}(\mathbf{x}'_i, \mathbf{v}_i) = \operatorname{dist}(\mathbf{x}'_i, \Lambda)$. Dále označme $\mathbf{x}_i = \mathbf{x}'_i - \mathbf{v}_i$. Protože Λ je aditivní grupou, platí

$$\operatorname{dist}(\mathbf{x}'_i, \Lambda) = \operatorname{dist}(\mathbf{x}_i, \Lambda) = \operatorname{dist}(\mathbf{x}_i, \mathbf{0}) = \|\mathbf{x}_i\|.$$

Protože $\mu(\Lambda) \cdot \overline{\mathcal{B}}_n$ je kompaktní množina, existuje konvergentní podposloupnost $\{\mathbf{x}_{i_j}\}_{j=1}^{\infty}$ posloupnosti $\{\mathbf{x}_i\}_{i=1}^{\infty}$ s limitou $\mathbf{h} = \lim_{j\to\infty} \mathbf{x}_{i_j}$. Platí $\|\mathbf{h}\| = \mu(\Lambda)$, protože $\lim_{i\to\infty} \|\mathbf{x}_i\| = \mu(\Lambda)$. Chceme ukázat, že $\operatorname{dist}(\mathbf{h}, \Lambda) = \mu(\Lambda)$. Pro spor ať existuje $\mathbf{w} \in \Lambda \setminus \{\mathbf{0}\}$ takový, že $\operatorname{dist}(\mathbf{h}, \mathbf{w}) = \mu(\Lambda) - \epsilon < \mu(\Lambda)$. Z konvergencí existuje $j \in \mathbb{N}$ takové, že $\|\mathbf{x}_{i_j}\| \geq \mu(\Lambda) - \frac{\epsilon}{3}$ a zároveň $\operatorname{dist}(\mathbf{x}_{i_j}, \mathbf{h}) \leq \frac{\epsilon}{3}$. Potom z trojúhelníkové nerovnosti máme

$$\operatorname{dist}(\mathbf{x}_{i_j}, \mathbf{w}) \leq \operatorname{dist}(\mathbf{x}_{i_j}, \mathbf{h}) + \operatorname{dist}(\mathbf{h}, \mathbf{w}) \leq \frac{\epsilon}{3} + \mu(\Lambda) - \epsilon = \mu(\Lambda) - \frac{2}{3}\epsilon,$$

ale zároveň platí $\operatorname{dist}(\mathbf{x}_{i_j}, \Lambda) = \|\mathbf{x}_{i_j}\| \geq \mu(\Lambda) - \frac{\epsilon}{3}$, tedy dostáváme spor a platí $\operatorname{dist}(\mathbf{h}, \Lambda) = \mu(\Lambda)$. □

Další cvičení nám ukazuje, že existují mříže, kde minimální vzdálenost může být blízko pokrývajícího poloměru. V důkazu budeme používat poznámku z [5], která říká, že pro každou mříž Λ splňující $\mu(\Lambda) > 2\lambda_1(\Lambda)$ existuje vektor $\mathbf{v} \in \Lambda$ takový, že vzdálenost $\frac{\mathbf{v}}{2}$ od mříže Λ je alespoň $\lambda_1(\Lambda)$. V důkazu této poznámky se využívá tvrzení z předchozího cvičení, proto jsem se rozhodl toto cvičení sem zařadit.

Cvičení 4. *Dokažte, že pro každou n-dimenzionální mříž Λ existuje mříž $\Lambda' \supseteq \Lambda$ splňující $\mu(\Lambda') \leq 2\lambda_1(\Lambda') = 2\lambda_1(\Lambda)$.*

Důkaz. Budeme postupně budovat posloupnost mříží $\Lambda_i \supseteq \Lambda_{i-1} \supseteq \cdots \supseteq \Lambda_0$ se stejnou minimální vzdáleností. Zvolme $\Lambda_0 = \Lambda$. Dále předpokládejme, že již máme posloupnost $\Lambda_i \supseteq \cdots \supseteq \Lambda_0$. Pokud platí $\mu(\Lambda_i) \leq 2\lambda_1(\Lambda_i)$, zvolíme $\Lambda' = \Lambda_i$ a jsme hotovi. V opačném případě existuje z poznámky výše vektor $\mathbf{v} \in \Lambda_i$ takový, že vzdálenost $\frac{\mathbf{v}}{2}$ od Λ_i je alespoň $\lambda_1(\Lambda_i)$. Zvolíme $\Lambda_{i+1} = \Lambda_i \cup (\Lambda_i + \frac{\mathbf{v}}{2})$. Ze cvičení 2 víme, že $\lambda_1(\Lambda_{i+1}) = \lambda_1(\Lambda_i)$ a $\det(\Lambda_{i+1}) = \det(\Lambda_i)/2$. Kdyby pro každé i nastala druhá možnost, dostali bychom spor s důsledkem 5, protože bychom pro fixní minimální vzdálenost našli mříž s libovolně malým determinantem. Tedy pro nějaké i nastane první možnost a jsme hotovi. □

2.3 Problémy na mřížích

Dále definujeme základní mřížové problémy. V redukcích se nejčastěji objevují aproximační varianty těchto problémů.

Definice 10 (*Shortest vector problem*)**.** *Mějme funkci $\gamma : \mathbb{N} \to \mathbb{R}$ splňující $\gamma(n) \geq 1$ pro každé n.*

- SVP*: Vstupem je báze $\mathbf{B}$ n-dimenzionální mříže $\Lambda = \mathcal{L}(\mathbf{B})$. Úkolem je najít nejkratší nenulový vektor této mříže, neboli vektor $\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}$ splňující $\|\mathbf{v}\| = \lambda_1(\Lambda)$.*
- SVP$_\gamma$*: Vstupem je báze $\mathbf{B}$ n-dimenzionální mříže $\Lambda = \mathcal{L}(\mathbf{B})$. Úkolem je aproximovat nejkratší nenulový vektor této mříže s faktorem $\gamma(n)$, neboli najít vektor $\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}$ splňující $\|\mathbf{v}\| \leq \gamma(n) \cdot \lambda_1(\Lambda)$.*
- GapSVP$_\gamma$*: Vstupem je dvojice $(\mathbf{B}, d)$, kde $\mathbf{B}$ je báze n-dimenzionální mříže $\Lambda = \mathcal{L}(\mathbf{B})$ a $d > 0$ je reálné číslo. Úkolem je rozhodnout, zda $\lambda_1(\Lambda) \leq d$ nebo $\lambda_1(\Lambda) > \gamma(n) \cdot d$. V případě, kdy $d < \lambda_1(\Lambda) \leq \gamma(n) \cdot d$, je jakákoliv odpověď přípustná.*

Mezera mezi d a $\gamma(n) \cdot d$ u verze GapSVP_γ odpovídá aproximaci minimální vzdálenosti na faktor $\gamma(n)$.

Pro naši redukci budeme potřebovat speciální verzi problému GapSVP_γ [2], která není těžší než klasická verze. Na druhou stranu není znám klasický ani kvantový algoritmus, který by byl schopný efektivně řešit tuto potenciálně lehčí variantu pro vhodné volby γ a ζ.

Definice 11 (ζ-to-γ-GapSVP)**.** *Mějme dvě funkce $\zeta(n) \geq \gamma(n) \geq 1$. Vstupem pro $\mathrm{GapSVP}_{\zeta,\gamma}$ je dvojice $(\mathbf{B}, d)$ splňující:*

1. *$\mathbf{B}$ je báze n-dimenzionální mříže $\Lambda = \mathcal{L}(\mathbf{B})$, pro kterou platí $\lambda_1(\Lambda) \leq \zeta(n)$,*
2. *$\min_i \|\widetilde{\mathbf{b}}_i\| \geq 1$,*
3. *$1 \leq d \leq \zeta(n)/\gamma(n)$.*

Úkolem je rozhodnout, zda $\lambda_1(\Lambda) \leq d$ nebo $\lambda_1(\Lambda) > \gamma(n) \cdot d$. V případě, kdy $d < \lambda_1(\Lambda) \leq \gamma(n) \cdot d$, je jakákoliv odpověď přípustná.

Z lemmatu 2 víme, že druhá podmínka implikuje $\lambda_1(\Lambda) \geq 1$, což můžeme uvažovat bez újmy na obecnosti, protože jinak můžeme vhodně přenásobit vektory báze tak, aby tato podmínka platila. Třetí podmínka je rovněž bez újmy na obecnosti, protože pokud d leží mimo daný interval, je problém za předpokladu první a druhé podmínky triviální. Zajímavá je tedy první podmínka. Nejprve poznamenejme, že pro $\zeta(n) \geq 2^{n/2}$ je $\mathrm{GapSVP}_{\zeta,\gamma}$ problém ekvivalentní standardnímu GapSVP_γ problému. Libovolnou bázi $\mathbf{B'}$ můžeme v polynomiálním čase zredukovat na jinou bázi $\mathbf{B}$ stejné mříže Λ pomocí algoritmu LLL [3, Kapitola 2]. Pro takto zredukovanou bázi poté platí

$$\lambda_1(\Lambda) \leq \|\mathbf{b}_1\| \leq 2^{n/2} \cdot \min_i \|\widetilde{\mathbf{b}}_i\|.$$

Nechť tedy máme instanci $(\mathbf{B'}, d)$ problému GapSVP_γ a jsme schopni řešit instance problému $\mathrm{GapSVP}_{\zeta,\gamma}$ pro $\zeta(n) \geq 2^{n/2}$. Bázi $\mathbf{B'}$ nejprve zredukujeme pomocí LLL algoritmu zmíněného výše na bázi $\mathbf{B}$ stejné mříže Λ. Uvažujme nyní bázi $\mathbf{C} = \mathbf{B}/\min_i \|\widetilde{\mathbf{b}}_i\|$ nové mříže Λ'. Tato báze splňuje $\min_i \|\widetilde{\mathbf{c}}_i\| = 1$ a navíc platí

$$\lambda_1(\Lambda') = \frac{\lambda_1(\Lambda)}{\min_i \|\widetilde{\mathbf{b}}_i\|} \leq 2^{n/2},$$

protože $\min_i \|\widetilde{\mathbf{b}}_i\| \cdot \lambda_1(\Lambda') = \lambda_1(\Lambda)$. Označme $d' = d/\min_i \|\widetilde{\mathbf{b}}_i\|$. Pokud $d' < 1$, potom určitě neplatí $\lambda_1(\Lambda') \leq d'$, protože $\lambda_1(\Lambda') \geq 1$. Tedy přenásobením výrazem $\min_i \|\widetilde{\mathbf{b}}_i\|$ dostaneme, že neplatí ani $\lambda_1(\Lambda) \leq d$. Tedy můžeme odpovědět, že $\lambda_1(\Lambda) > \gamma(n) \cdot d$. Analogicky, pokud $\gamma(n) \cdot d' > \zeta(n)$, potom určitě neplatí, že $\lambda_1(\Lambda) > \gamma(n) \cdot d$, a tedy můžeme odpovědět, že $\lambda_1(\Lambda) \leq d$. Nakonec předpokládejme, že

$$1 \leq d' \leq \zeta(n)/\gamma(n).$$

Potom je dvojice $(\mathbf{C}, d')$ korektním vstupem pro $\mathrm{GapSVP}_{\zeta,\gamma}$ problém. Vyřešíme tedy $\mathrm{GapSVP}_{\zeta,\gamma}$ pro $(\mathbf{C}, d')$. Pokud $\lambda_1(\Lambda') \leq d'$, potom přenásobením nerovnosti výrazem $\min_i \|\widetilde{\mathbf{b}}_i\|$ dostaneme, že $\lambda_1(\Lambda) \leq d$. Analogicky pokud $\lambda_1(\Lambda') > \gamma(n) \cdot d'$, potom $\lambda_1(\Lambda) > \gamma(n) \cdot d$. Tedy jsme vyřešili GapSVP_γ pro daný vstup.

První podmínka je tedy zajímavější v případě, kdy $\zeta(n) = \text{poly}(n)$. Nicméně i v tomto případě pracují všechny známé algoritmy řešící $\text{GapSVP}_{\zeta,\gamma}$ nejlépe v čase $2^{\Omega(n)}$, dokonce i pro volbu $\zeta(n) = 2 \cdot \gamma(n)$.

V naší redukci budou hrát roli ještě následující dva problémy, které jsou speciální verzí problému nejbližšího vektoru.

Definice 12 (*Bounded distance decoding*)**.** *Buď $p \geq 2$ celé a $d > 0$ reálné. Dále buď Λ n-dimenzionální mříž splňující $d < \lambda_1(\Lambda)/2$. Mějme k dispozici nějakou bázi $\mathbf{B}$ mříže Λ.*

- $\text{BDD}_{\Lambda,d}$*: Vstupem je bod $\mathbf{x} \in \mathbb{R}^n$ ve vzdálenosti nejvýše d od mříže Λ. Úkolem je najít jednoznačně určený vektor $\mathbf{v} \in \Lambda$ nejblíže k $\mathbf{x}$.*
- $\text{BDD}^{(p)}_{\Lambda,d}$*: Vstupem je bod $\mathbf{x} \in \mathbb{R}^n$ ve vzdálenosti nejvýše d od mříže Λ. Úkolem je najít $\mathbf{B}^{-1}\mathbf{v} \bmod p \in \mathbb{Z}_p^n$, kde $\mathbf{v} \in \Lambda$ je jednoznačně určený vektor nejblíže k $\mathbf{x}$.*

Jinými slovy, v problému $\text{BDD}^{(p)}_{\Lambda,d}$ je úkolem najít souřadnice vůči bázi $\mathbf{B}$ modulo p nejbližšího vektoru mříže Λ od bodu $\mathbf{x}$.

Nejbližší vektor $\mathbf{v} \in \Lambda$ je jednoznačně určený, protože $d < \lambda_1(\Lambda)/2$. Jinak bychom totiž měli dva různé vektory $\mathbf{v}_1, \mathbf{v}_2 \in \Lambda$ ve vzdálenosti ostře menší než $\lambda_1(\Lambda)/2$ od bodu $\mathbf{x}$. Jejich rozdíl je z definice vektor mříže, jehož norma je z trojúhelníkové nerovnosti ostře menší než $\frac{\lambda_1(\Lambda)}{2} + \frac{\lambda_1(\Lambda)}{2} = \lambda_1(\Lambda)$, což by byl spor. Jednoznačně určený nejbližší vektor mříže Λ od bodu $\mathbf{x}$ budeme značit $\kappa_\Lambda(\mathbf{x})$.

3. Problém LWE

3.1 Základní pojmy, pravděpodobnost

Pro konečnou množinu A nebo pro otevřenou kouli $A = \mathbf{c} + r \cdot \mathcal{B}_n$, kde $\mathbf{c} \in \mathbb{R}^n$ a $r > 0$ je reálné, budeme výrazem $\mathcal{U}(A)$ označovat rovnoměrné rozdělení pravděpodobnosti na A. Kvůli přehlednosti budeme někdy mlčky zaměňovat rozdělení pravděpodobnosti za náhodnou veličinu (nebo za náhodný vektor) mající toto rozdělení. Bude-li například χ_1 rozdělení pravděpodobnosti na $\mathbb{R}$ a bude-li $f : \mathbb{R} \to \mathbb{R}$ měřitelné zobrazení, potom výrazem „χ_2 je rozdělení $f(\chi_1)$“ máme na mysli, že χ_2 je rozdělení pravděpodobnosti, které má náhodná veličina $f(X)$, kde X je náhodná veličina mající rozdělení χ_1. Obecně, budou-li $\chi_1, \ldots, \chi_n$ rozdělení pravděpodobnosti a budeme-li provádět s těmito rozděleními operace, potom je implicitně provádíme s příslušnými náhodnými veličinami (popř. náhodnými vektory). Výrazem $a \leftarrow \chi$ budeme značit volbu hodnoty a z rozdělení pravděpodobnosti χ. To využijeme jednak při popisu konkrétního schématu, jednak při dokazování redukcí. V schématu budeme potřebovat zvolit například soukromý klíč, v redukcích budeme potřebovat zvolit vektory a transformovat je tak, aby jejich rozdělení bylo blízko nějakému ideálnímu požadovanému rozdělení. Bude-li χ rozdělení pravděpodobnosti na $A \subset \mathbb{R}$, potom výrazem χ^n máme na mysli rozdělení pravděpodobnosti na A^n, které má náhodný vektor $X = (X_1, \ldots, X_n)$, kde náhodné veličiny X_i jsou nezávislé a mají rozdělení χ.

Důležitými pravděpodobnostními rozděleními v našich redukcích je Gaussovo rozdělení a rozdělení z něho odvozená, která si nyní definujeme. Budeme vycházet z článku [1].

Definice 13 (Gaussova funkce)**.** *Buď $n \in \mathbb{N}$ a $r \in \mathbb{R}$, $r > 0$. Potom n-dimenzionální* Gaussovu funkci $\rho_r^{(n)} : \mathbb{R}^n \to \mathbb{R}$ *s parametrem r definujeme jako*

$$\rho_r^{(n)}(\mathbf{x}) = \exp\left(-\pi\left(\frac{\|\mathbf{x}\|}{r}\right)^2\right).$$

Výrazem $\rho_r(A)$ máme na mysli $\sum_{\mathbf{a}\in A} \rho_r(\mathbf{a})$ pro $A \subset \mathbb{R}^n$ spočetnou diskrétní. Platí, že $\int_{\mathbb{R}^n} \rho_r^{(n)}(\mathbf{x})\, \mathrm{d}\mathbf{x} = r^n$. Můžeme tedy definovat spojité Gaussovo pravděpodobnostní rozdělení na $\mathbb{R}^n$.

Definice 14 (Gaussovo rozdělení)**.** Gaussovo rozdělení $D_r^{(n)}$ *definujeme jako spojité rozdělení pravděpodobnosti s hustotou*

$$D_r^{(n)}(\mathbf{x}) = \frac{\rho_r^{(n)}(\mathbf{x})}{r^n} \quad \forall \mathbf{x} \in \mathbb{R}^n.$$

Pokud bude dimenze n jasná z kontextu, budeme místo $\rho_r^{(n)}$ psát zkráceně ρ_r a podobně pro $D_r^{(n)}$. Rozdělení pravděpodobnosti $D_r^{(n)}$ a $\mathcal{U}(\mathbf{c} + r \cdot \mathcal{B}_n)$ je možné aproximovat s libovolně velkou přesností. V této práci budeme pro jednoduchost předpokládat, že máme k dispozici efektivní algoritmus, který nám vrací vektory z těchto rozdělení přesně. [2]. Následující dvě rozdělení jsou odvozená z Gaussova rozdělení.

- *Diskrétní Gaussovo rozdělení*
  Buď $A \subset \mathbb{R}^n$ spočetná diskrétní a $r > 0$ reálné. Diskrétní Gaussovo rozdělení $D_{A,r}$ na A s parametrem r definujeme jako

$$D_{A,r}(\mathbf{x}) = \frac{\rho_r(\mathbf{x})}{\rho_r(A)} \quad \forall \mathbf{x} \in A.$$

- *Gaussovo rozdělení na kružnici*
  Pro $\alpha > 0$ reálné definujeme rozdělení pravděpodobnosti Ψ_α na $\mathbb{T}$ jako rozdělení $D_\alpha^{(1)}$ modulo 1. Tedy Ψ_α je spojité rozdělení pravděpodobnosti s hustotou

$$\Psi_\alpha(r) = \sum_{k=-\infty}^{\infty} \frac{1}{\alpha} \cdot \exp\left(-\pi \left(\frac{r-k}{\alpha}\right)^2\right) \quad \forall r \in [0,1).$$

V naší práci budeme při Gaussově diskrétním rozdělení uvažovat $A = \Lambda + \mathbf{c}$, kde Λ je n-dimenzionální mříž a $\mathbf{c} \in \mathbb{R}^n$.

V roce 2007 představili Regev a Micciancio [6] nový parametr mříže, nazývaný smoothing parametr. Ten hraje důležitou roli při práci s pravděpodobnostními rozděleními v souvislosti s mřížemi.

Definice 15 (Smoothing parametr)**.** *Buď Λ n-dimenzionální mříž a $\epsilon > 0$ reálné.* Smoothing parametr $\eta_\epsilon(\Lambda)$ *mříže Λ definujeme jako nejmenší $r > 0$ takové, že*

$$\rho_{1/r}(\Lambda^* \setminus \{\mathbf{0}\}) \leq \epsilon.$$

V Regevově redukci využijeme následující lemma.

Lemma 8. *Pro každé $c > 0$ reálné a pro každou mříž Λ platí $\eta_\epsilon(c \cdot \Lambda) = c \cdot \eta_\epsilon(\Lambda)$.*

Důkaz. Plyne ze vztahů $(c\Lambda)^* = \frac{1}{c}\Lambda^*$ a $\rho_{s/r}(\mathbf{x}) = \rho_s(r \cdot \mathbf{x})$. □

Později budeme potřebovat následující vztah mezi smoothing parametrem a minimální vzdáleností mříže.

Lemma 9 ([6, Lemma 3.2])**.** *Pro každou n-dimenzionální mříž Λ platí*

$$\eta_\epsilon(\Lambda) \leq \frac{\sqrt{n}}{\lambda_1(\Lambda^*)},$$

kde $\epsilon = 2^{-n}$.

Jak shrnuje následující lemma, smoothing parametr se nám hodí především při práci s Gaussovou funkcí. Lemma budeme potřebovat při aproximování rovnoměrného rozdělení pravděpodobnosti na $\mathbb{Z}_p^n$.

Lemma 10 ([1, Claim 3.8])**.** *Nechť Λ je n-dimenzionální mříž. Nechť jsou dále $r \geq \eta_\epsilon(\Lambda)$ a $\epsilon > 0$ reálná a $\mathbf{c} \in \mathbb{R}^n$. Potom*

$$\rho_r(\Lambda + \mathbf{c}) \in (1 \pm \epsilon) \cdot r^n \det(\Lambda^*).$$

3.2 Problém LWE

Jak jsme zmínili v úvodu, v problému LWE jde neformálně o řešení soustavy zašumělých lineárních rovnic. Nejprve definujeme dvě rozdělení pravděpodobnosti, která poté použijeme pro definici problému LWE. Už z těchto rozdělení lze vidět, co myslíme zašumělými rovnicemi. První rozdělení se více hodí pro práci s redukcemi, druhé na aplikace. Budeme vycházet především z článků [1, 2].

Definice 16 (LWE distribuce)**.** *Buď n a p přirozená čísla taková, že $p \geq 2$. Dále buď $\mathbf{s} \in \mathbb{Z}_p^n$.*

- spojitá LWE distribuce
  Buď ϕ rozdělení pravděpodobnosti na $\mathbb{T}$. Potom definujeme rozdělení pravděpodobnosti $A_{\mathbf{s},\phi}$ na $\mathbb{Z}_p^n \times \mathbb{T}$ následujícím způsobem. Zvolíme $\mathbf{a} \leftarrow \mathcal{U}(\mathbb{Z}_p^n)$ a $e \leftarrow \phi$. Výstupem bude dvojice $(\mathbf{a}, \langle \mathbf{a},\mathbf{s} \rangle / p + e \bmod 1)$.

- diskrétní LWE distribuce
  Buď χ rozdělení pravděpodobnosti na $\mathbb{Z}_p$. Potom definujeme rozdělení pravděpodobnosti $A_{\mathbf{s},\chi}$ na $\mathbb{Z}_p^n \times \mathbb{Z}_p$ následujícím způsobem. Zvolíme $\mathbf{a} \leftarrow \mathcal{U}(\mathbb{Z}_p^n)$ a $e \leftarrow \chi$. Výstupem bude dvojice $(\mathbf{a}, \langle \mathbf{a},\mathbf{s} \rangle + e \bmod p)$.

Nyní máme vše připraveno na to, abychom mohli definovat problém LWE a jeho varianty. Třetí a čtvrtá varianta v následující definici se hodí zejména při dokazování bezpečnosti konkrétních kryptosystémů. My je budeme chápat pouze intuitivně, protože jsme si formálně nedefinovali, co znamená, že algoritmus rozliší dvě rozdělení pravděpodobnosti s nezanedbatelnou výhodou. Neformálně, pro útočníka, který neumí řešit decision-LWE$_{p,\chi}$ (resp. HNF-decision-LWE$_{p,\chi}$) problém, se chová rozdělení pravděpodobnosti $A_{\mathbf{s},\chi}$ pseudonáhodně.

Definice 17 (Problém LWE)**.** *Buď $p = p(n)$ celé.*

- search-LWE$_{p,\phi}$, spojitá verze
  Nechť ϕ je pravděpodobnostní rozdělení na $\mathbb{T}$. Vstupem je polynomiálně mnoho dvojic z rozdělení $A_{\mathbf{s},\phi}$ pro $\mathbf{s} \in \mathbb{Z}_p^n$. Úkolem je zjistit $\mathbf{s}$. Řekneme, že algoritmus $\mathcal{A}$ řeší problém search-LWE$_{p,\phi}$*, pokud pro každé $\mathbf{s}$ vrátí toto $\mathbf{s}$ s velkou pravděpodobností.*

- search-LWE$_{p,\chi}$, diskrétní verze
  Nechť χ je pravděpodobnostní rozdělení na $\mathbb{Z}_p$. Vstupem je polynomiálně mnoho dvojic z rozdělení $A_{\mathbf{s},\chi}$ pro $\mathbf{s} \in \mathbb{Z}_p^n$. Úkolem je zjistit $\mathbf{s}$. Řekneme, že algoritmus $\mathcal{A}$ řeší problém search-LWE$_{p,\chi}$*, pokud pro každé $\mathbf{s}$ vrátí toto $\mathbf{s}$ s velkou pravděpodobností.*

- decision-LWE$_{p,\chi}$, diskrétní verze
  Nechť χ je pravděpodobnostní rozdělení na $\mathbb{Z}_p$. Řekneme, že algoritmus $\mathcal{A}$ řeší problém decision-LWE$_{p,\chi}$*, pokud s nezanedbatelnou výhodou rozliší rozdělení pravděpodobnosti $A_{\mathbf{s},\chi}$ a $\mathcal{U}(\mathbb{Z}_p^n \times \mathbb{Z}_p)$ pro $\mathbf{s} \leftarrow \mathcal{U}(\mathbb{Z}_p^n)$.*

- HNF-decision-LWE$_{p,\chi}$, diskrétní verze
  Nechť χ je pravděpodobnostní rozdělení na $\mathbb{Z}_p$. Řekneme, že algoritmus $\mathcal{A}$ řeší problém HNF-decision-LWE$_{p,\chi}$*, pokud s nezanedbatelnou výhodou rozliší rozdělení pravděpodobnosti $A_{\mathbf{s},\chi}$ a $\mathcal{U}(\mathbb{Z}_p^n \times \mathbb{Z}_p)$ pro $\mathbf{s} \leftarrow \chi^n$.*

Zdali se jedná o spojitou nebo diskrétní verzi, poznáme z příslušného chybového rozdělení. Budeme používat ϕ pro spojitou verzi a χ pro diskrétní. V definici je p celočíselnou funkcí proměnné $n \in \mathbb{N}$, která je hlavním parametrem problému. Počet dvojic z rozdělení $A_{\mathbf{s},\phi}$, pravděpodobnost úspěchu i časová složitost jsou funkcemi proměnné n. Rozdělení pravděpodobnosti ϕ, χ také závisí na hlavním parametru n, tedy se mohou lišit pro různá n. Uveďme konkrétní příklad.

Příklad. Buď $p = n^2$, $\chi = \lfloor D_{n^2/5} \rceil \bmod p$, $P(n) = 2n^3 + 2$ a $Q(n) = 3n^7$. Buď dále $\mathcal{A}$ algoritmus, který pro každé $n \in \mathbb{N}$ pracuje v čase nejvíce $P(n)$ a který na vstupu $Q(n)$ dvojic z rozdělení $A_{\mathbf{s},\phi}$ vrátí $\mathbf{s}$ s pravděpodobností alespoň $1-2^{-n}$ pro libovolné $\mathbf{s} \in \mathbb{Z}_p^n$. Potom o takovém algoritmu $\mathcal{A}$ řekneme, že efektivně řeší problém search-LWE$_{p,\chi}$.

V této práci budeme redukovat mřížové problémy na problém search-LWE$_{p,\phi}$, ale na aplikace se více hodí problém HNF-decision-LWE$_{p,\chi}$, protože za prvé potřebujeme, aby se jednalo o rozhodovací verzi, za druhé chceme pracovat v $\mathbb{Z}_p$ a za třetí požadujeme, aby složky vektoru $\mathbf{s}$ určujícího rozdělení $A_{\mathbf{s},\chi}$ byly koncentrovány kolem nuly, což můžeme zajistit vhodnou volbou rozdělení pravděpodobnosti χ. Pro p prvočíslo a vhodné chybové rozdělení platí, že problém HNF-decision-LWE$_{p,\chi}$ není těžší než problém search-LWE$_{p,\phi}$.

Lemma 11. *Nechť $p = p(n)$ je prvočíslo a $\alpha = \alpha(n) \in (0,1)$ je reálné. Pokud existuje pravděpodobnostní polynomiální algoritmus $\mathcal{A}$, který řeší problém HNF-decision-LWE$_{p,\chi}$ pro $\chi = \lfloor D_{\alpha p} \rceil \bmod p$, potom existuje pravděpodobnostní polynomiální algoritmus $\mathcal{B}$, který řeší problém search-LWE$_{p,\Psi_\alpha}$.*

Důkaz. Kombinace [1, Lemma 4.4] a [7, Lemma 2]. □

3.3 Statistická vzdálenost

V redukcích často musíme nahradit rozdělení pravděpodobnosti nějakou jeho aproximací a potřebujeme vědět, jak se změní chování algoritmu pracujícího s těmito rozděleními. K tomu nám slouží pojem statistické vzdálenosti, který si nyní zadefinujeme. Začneme obecnou definicí, ze které jsou lépe vidět nějaké vlastnosti, a poté si ukážeme ekvivalentní definice pro diskrétní a spojitá rozdělení pravděpodobnosti, které se více hodí na výpočet. V této sekci budeme čerpat především z knihy [3, Kapitola 8]. Na rozdíl od [3] se ale pokusíme definici a tvrzení zobecnit pro libovolná rozdělení pravděpodobnosti a ne pouze pro diskrétní, protože v redukcích budeme pracovat například se spojitými rozděleními pravděpodobnosti. Připomeňme, že budeme někdy zaměňovat rozdělení pravděpodobnosti s náhodným vektorem mající toto rozdělení. Teorii v této části popíšeme obecně pro rozdělení pravděpodobnosti, neboli pro pravděpodobnostní míry. Protože ji ale nakonec aplikujeme na pravděpodobnostní algoritmy, na které se budeme dívat jako na náhodné veličiny (nebo náhodné vektory), budeme používat značení $\Pr[X \in A]$ místo $X(A)$ i pro rozdělení pravděpodobnosti X a jev A.

Definice 18 (Statistická vzdálenost)**.** *Nechť jsou X, Y dvě rozdělení pravděpodobnosti na stejném prostoru Ω a buď $\mathcal{F}$ množina všech možných jevů. Potom statistickou vzdálenost mezi X, Y definujeme jako*

$$\Delta(X,Y) = \sup_{A \in \mathcal{F}} |\Pr[X \in A] - \Pr[Y \in A]| .$$

Statistickou vzdáleností dvou náhodných vektorů budeme myslet statistickou vzdálenost jejich rozdělení. Jinými slovy, jedná se o maximální možný rozdíl pravděpodobností, které mohou X, Y přiřadit stejnému jevu. Vidíme, že pro každý jev $A \in \mathcal{F}$ platí

$$\Pr[X \in A] \geq \Pr[Y \in A] - \Delta(X, Y).$$

Tedy pokud se na X, Y budeme dívat jako na rozdělení výstupů dvou pravděpodobnostních algoritmů $\mathcal{A}_X, \mathcal{A}_Y$, potom je pravděpodobnost, že $\mathcal{A}_X$ vrátí správné řešení s, což označíme $\Pr[\mathcal{A}_X = s]$, alespoň $\Pr[\mathcal{A}_Y = s] - \Delta(\mathcal{A}_X, \mathcal{A}_Y)$. Víme-li tedy statistickou vzdálenost mezi $\mathcal{A}_X, \mathcal{A}_Y$, umíme odhadnout, s jakou pravděpodobností nám algoritmus $\mathcal{A}_X$ vrátí správné řešení s v porovnání s algoritmem $\mathcal{A}_Y$.

Mějme nyní dvě diskrétní rozdělení pravděpodobnosti X, Y na Ω. Potom jsme mohli jejich statistickou vzdálenost definovat jako

$$\Delta(X, Y) = \frac{1}{2} \sum_{\omega \in \Omega} \left| \Pr[X = \omega] - \Pr[Y = \omega] \right|.$$

Podobně, mějme dvě spojitá rozdělení pravděpodobnosti X, Y na $\mathbb{R}^n$ s hustotami ϕ_1, ϕ_2. Jejich statistickou vzdálenost jsme mohli definovat jako

$$\Delta(X, Y) = \frac{1}{2} \int_{\mathbb{R}^n} |\phi_1(\mathbf{x}) - \phi_2(\mathbf{x})| \, d\mathbf{x}.$$

Výše zmíněné definice pro speciální případy lze nalézt například v [6]. Uveďme příklad pro diskrétní rozdělení pravděpodobnosti.

Příklad. Buď X rovnoměrné rozdělení na množině $\{1, 2, 3, 4\}$ a buď Y rozdělení splňující

$$\Pr[Y = 1] = \frac{1}{12}, \qquad \Pr[Y = 2] = \frac{1}{6}, \qquad \Pr[Y = 3] = \frac{1}{4}, \qquad \Pr[Y = 4] = \frac{1}{2}.$$

Potom podle druhé definice máme

$$\Delta(X, Y) = \frac{1}{2} \left(\frac{2}{12} + \frac{1}{12} + 0 + \frac{3}{12} \right) = \frac{1}{4},$$

což dle první definice odpovídá jevu $\{3, 4\}$, kdy

$$\Pr[X \in \{3{,}4\}] = \frac{1}{2}, \qquad \Pr[Y \in \{3{,}4\}] = \frac{3}{4}, \qquad \left| \frac{1}{2} - \frac{3}{4} \right| = \frac{1}{4}.$$

Bez důkazu zmiňme, že statistická vzdálenost splňuje trojúhelníkovou nerovnost, neboli pro každé tři rozdělení pravděpodobnosti X, Y, Z na stejném prostoru Ω platí, že

$$\Delta(X, Z) \leq \Delta(X, Y) + \Delta(Y, Z).$$

V další části budeme chtít rozdělení pravděpodobnosti skládat za sebe, například abychom mohli mluvit o rozdělení k dvojic z $A_{\mathbf{s},\phi}$, kdy jsou volby jednotlivých dvojic nezávislé. To si nyní formálně definujeme. Nechť $(\Omega_1, \mathcal{F}_1, P_1), (\Omega_2, \mathcal{F}_2, P_2)$ jsou dva pravděpodobnostní prostory a buď $(\Omega_1 \times \Omega_2, \mathcal{F}_1 \otimes \mathcal{F}_2)$ měřitelný prostor, kde

$$\mathcal{F}_1 \otimes \mathcal{F}_2 = \sigma(A \times B : \ A \in \mathcal{F}_1, B \in \mathcal{F}_2).$$

Potom existuje právě jedna pravděpodobnost P na $(\Omega_1 \times \Omega_2, \mathcal{F}_1 \otimes \mathcal{F}_2)$ splňující

$$P(A \times B) = P_1(A) \cdot P_2(B) \quad \forall A \in \mathcal{F}_1, B \in \mathcal{F}_2.$$

Výrazem $\sigma(\mathcal{S})$ zde značíme nejmenší sigma algebru obsahující množinový systém $\mathcal{S}$. Detaily lze nalézt například v [8]. Budou-li X, Y dvě rozdělení pravděpodobnosti, pak výrazem (X, Y) máme na mysli právě výše zmíněnou konstrukci, kde $P_1 = X$ a $P_2 = Y$. Analogicky pro více rozdělení.

Další lemma se hodí v situacích, kdy chceme analyzovat pravděpodobnostní algoritmus. Na rozdělení pravděpodobnosti Z z lemmatu se totiž můžeme dívat jako na náhodné volby pravděpodobnostního algoritmu. Protože kompletní důkaz se všemi detaily je příliš technický pro účely této práce, tak uvedeme pouze část důkazu pro jevy speciálního tvaru.

Lemma 12. *Buď X, Y dvě rozdělení pravděpodobnosti na Ω a buď Z rozdělení pravděpodobnosti na Υ. Potom platí*

$$\Delta((X, Z), (Y, Z)) = \Delta(X, Y).$$

Důkaz. Pro spor předpokládejme, že to neplatí. Nejprve se podíváme na situaci, kdy

$$\Delta((X, Z), (Y, Z)) > \Delta(X, Y).$$

Tedy existuje jev F na $\Omega \times \Upsilon$ takový, že

$$|\Pr[(X, Z) \in F] - \Pr[(Y, Z) \in F]| > \Delta(X, Y).$$

Pro jednoduchost předpokládejme, že $F = A \times B$, kde A je jev na Ω a B je jev na Υ. Nicméně také platí, že

$$\begin{aligned} &|\Pr[(X, Z) \in A \times B] - \Pr[(Y, Z) \in A \times B]| \\ &= \Pr[Z \in B] \cdot |\Pr[X \in A] - \Pr[Y \in A]| \\ &\leq |\Pr[X \in A] - \Pr[Y \in A]| \\ &\leq \Delta(X, Y). \end{aligned}$$

Naopak pokud

$$\Delta((X, Z), (Y, Z)) < \Delta(X, Y),$$

pak existuje jev A na Ω takový, že

$$|\Pr[X \in A] - \Pr[Y \in A]| > \Delta((X, Z),(Y, Z)).$$

To je ovšem spor, protože vezmeme-li za jev B celé Υ, dostaneme, že

$$|\Pr[(X, Z) \in A \times B] - \Pr[(Y, Z) \in A \times B]| = |\Pr[X \in A] - \Pr[Y \in A]|.$$

□

Bude se nám hodit také následující lemma, které plyne z trojúhelníkové nerovnosti pro statistickou vzdálenost a z předchozího lemmatu.

Lemma 13. *Buď X_i, Y_i rozdělení pravděpodobnosti na Ω_i pro $i = 1, \ldots, k$. Potom platí*

$$\Delta((X_1, \ldots, X_k),(Y_1, \ldots, Y_k)) \leq \sum_{i=1}^{k} \Delta(X_i, Y_i).$$

Nám se lemma bude hodit v situacích, kdy $X_i = A_{\mathbf{s},\phi}$ a Y_i je jeho aproximace taková, že $\Delta(X_i, Y_i) = \text{negl}(n)$, a $k = \text{poly}(n)$. Potom $(X_1, \ldots, X_k) = X$ odpovídá rozdělení k dvojic z $A_{\mathbf{s},\phi}$, a pro aproximaci $(Y_1, \ldots, Y_k) = Y$ platí

$$\Delta(X, Y) \leq \text{poly}(n) \cdot \text{negl}(n) = \text{negl}(n).$$

Kromě lemmat z [3] přidáme ještě jedno vlastní, které budeme v Regevově redukci potřebovat, abychom mohli formálně pracovat se statistickou vzdáleností, a nikde jsme ho nenašli.

Lemma 14. *Buď $\epsilon > 0$. Nechť X, Y jsou dvě rozdělení pravděpodobnosti na $\Omega \times \Upsilon$, kde Ω je konečná. Označme X_1 (resp. Y_1) rozdělení první složky X (resp. Y) na Ω a předpokládejme, že $\Delta(X_1, Y_1) \leq \epsilon_1$. Dále pro $\omega \in \Omega$ označme X_ω (resp. Y_ω) rozdělení druhé složky X (resp. Y) na Υ podmíněné na $X_1 = \omega$ (resp. na $Y_1 = \omega$) a předpokládejme, že pro každé $\omega \in \Omega$ platí $\Delta(X_\omega, Y_\omega) \leq \epsilon_2$. Potom platí, že*

$$\Delta(X, Y) \leq 2\epsilon_1 + \epsilon_2.$$

Důkaz. Buď A jev na $\Omega \times \Upsilon$. Potom

$$A = \bigcup_{\omega \in \Omega} \omega \times A_\omega,$$

kde A_ω jsou jevy na Υ. Platí

$$\Pr[X \in A] = \sum_{\omega \in \Omega} \Pr[X_1 = \omega] \cdot \Pr[X_\omega \in A_\omega].$$

Analogicky pro $\Pr[Y \in A]$. Místo $\Pr[Z \in B]$ a $\Pr[Z = \omega]$ budeme psát někdy zkráceně $Z(B)$ a $Z(\omega)$. Přičtením vhodné nuly, z trojúhelníkové nerovnosti, předpokladu na $\Delta(X_\omega, Y_\omega)$ a definice pravděpodobnosti dostaneme, že

$$\begin{aligned}
&\left|X_1(\omega) \cdot X_\omega(A_\omega) - Y_1(\omega) \cdot Y_\omega(A_\omega)\right| \\
&= \left|X_1(\omega) \cdot X_\omega(A_\omega) - X_1(\omega) \cdot Y_\omega(A_\omega) + X_1(\omega) \cdot Y_\omega(A_\omega) - Y_1(\omega) \cdot Y_\omega(A_\omega)\right| \\
&\leq X_1(\omega) \cdot \left|X_\omega(A_\omega) - Y_\omega(A_\omega)\right| + Y_\omega(A_\omega) \cdot \left|X_1(\omega) - Y_1(\omega)\right| \\
&\leq \epsilon_2 \cdot X_1(\omega) + Y_\omega(A_\omega) \cdot \left|X_1(\omega) - Y_1(\omega)\right| \\
&\leq \epsilon_2 \cdot X_1(\omega) + \left|X_1(\omega) - Y_1(\omega)\right|
\end{aligned}$$

Tedy máme, že

$$\begin{aligned}
|\Pr[X \in A] - \Pr[Y \in A]| &= \left|\sum_{\omega \in \Omega} X_1(\omega) \cdot X_\omega(A_\omega) - Y_1(\omega) \cdot Y_\omega(A_\omega)\right| \\
&\leq \sum_{\omega \in \Omega} \epsilon_2 \cdot X_1(\omega) + \left|X_1(\omega) - Y_1(\omega)\right| \\
&= \epsilon_2 \cdot \sum_{\omega \in \Omega} X_1(\omega) + \sum_{\omega \in \Omega} \left|X_1(\omega) - Y_1(\omega)\right| \\
&= \epsilon_2 + \sum_{\omega \in \Omega} \left|X_1(\omega) - Y_1(\omega)\right| \\
&= \epsilon_2 + 2 \cdot \Delta(X_1, Y_1) \\
&\leq 2\epsilon_1 + \epsilon_2.
\end{aligned}$$

Odtud plyne tvrzení. □

Klíčová pro nás bude následující vlastnost, která říká, že se statistická vzdálenost nemůže zvětšit aplikováním zobrazení f.

Tvrzení 15. *Buď X, Y dvě rozdělení pravděpodobnosti na Ω. Buď f měřitelné zobrazení z Ω do Υ. Potom platí*

$$\Delta(f(X), f(Y)) \leq \Delta(X, Y),$$

kde $f(X)$ (resp. $f(Y)$) je rozdělení pravděpodobnosti na Υ definované jako

$$\Pr[f(X) \in A] = \Pr[X \in f^{-1}(A)]$$

pro každý jev A na Υ.

Důkaz. Pro spor předpokládejme, že

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

Tedy existuje jev A na Υ takový, že

$$|\Pr[f(X) \in A] - \Pr[f(Y) \in A]| > \Delta(X, Y).$$

Z definice ale plyne, že

$$|\Pr[f(X) \in A] - \Pr[f(Y) \in A]| = \left|\Pr[X \in f^{-1}(A)] - \Pr[Y \in f^{-1}(A)]\right|,$$

a protože $f^{-1}(A)$ je jev na Ω, platí

$$\left|\Pr[X \in f^{-1}(A)] - \Pr[Y \in f^{-1}(A)]\right| \leq \Delta(X, Y),$$

čímž dostáváme spor. □

Předchozí tvrzení se pokusíme zobecnit i pro pravděpodobnostní algoritmy, které se objevují v redukcích. Mějme pravděpodobnostní algoritmus $\mathcal{A}$, který na vstupech z nějaké množiny Ω dělá maximálně c náhodných voleb, kde c je konstanta. Potom se můžeme na $\mathcal{A}$ dívat jako na deterministický algoritmus $\mathcal{A}'$, který kromě vstupu $\omega \in \Omega$ bere i $z \leftarrow Z$, kde Z je rozdělení pravděpodobnosti náhodných voleb. Budou-li tedy X, Y dvě rozdělení pravděpodobnosti na Ω, máme

$$\Delta(\mathcal{A}(X), \mathcal{A}(Y)) = \Delta(\mathcal{A}'(X, Z), \mathcal{A}'(Y, Z)) \leq \Delta((X,Z),(Y, Z)) = \Delta(X, Y).$$

Tedy pokud X, Y budou blízké, pak musí být blízké i rozdělení výstupů algoritmu $\mathcal{A}$ na vstupech z X, Y. Bude-li například X rozdělení pravděpodobnosti k dvojic z $\chi = A_{\mathbf{s},\phi}$, Y jeho aproximace v zanedbatelné statistické vzdálenosti a $\mathcal{A}$ pravděpodobnostní algoritmus řešící problém search-LWE$_{p,\chi}$, potom $\mathcal{A}$ najde $\mathbf{s}$ s velkou pravděpodobností i na vstupu k dvojic z rozdělení Y, protože

$$\Pr[\mathcal{A}(Y) = \mathbf{s}] \geq \Pr[\mathcal{A}(X) = \mathbf{s}] - \mathrm{negl}(n) = 1 - \mathrm{negl}(n) - \mathrm{negl}(n) = 1 - \mathrm{negl}(n).$$

Následující lemma odhaduje statistickou vzdálenost dvou rovnoměrných rozdělení na relativně blízkých koulích.

Lemma 16 ([2, Lemma 2.1]). *Nechť $c, d > 0$ jsou konstanty a buď $\mathbf{z} \in \mathbb{R}^n$ takový, že $\|\mathbf{z}\| \leq d$. Položme $d' = d \cdot \sqrt{n/(c \log n)}$. Potom platí*

$$\Delta(\mathcal{U}(d' \cdot \mathcal{B}_n), \mathcal{U}(\mathbf{z} + d' \cdot \mathcal{B}_n)) \leq 1 - 1/\mathrm{poly(n)}.$$

Mohlo by se zdát, že jsme si tolik nepomohli, protože $1 - 1/\mathrm{poly}(n)$ může být relativně blízko jedné. Nicméně důležité je, že vzdálenost od jedné je alespoň převrácená hodnota polynomu. Bude-li totiž pravděpodobnost úspěchu v nějakém pokusu například $1/n^3$ a opakujeme-li tento pokus n^4-krát, potom bude pravděpodobnost (za předpokladu, že pokusy jsou nezávislé), že alespoň jednou uspějeme, minimálně $1 - (1 - 1/n^3)^{n^4}$, což nám stačí, protože

$$(1 - 1/n^3)^{n^4} \approx e^{-n},$$

a tedy pravděpodobnost alespoň jednoho úspěchu bude velká. Navíc bude-li algoritmus vykonávající jeden pokus pracovat v polynomiálním čase, potom bude algoritmus vykonávající celý experiment pracovat také v polynomiálním čase, což stále považujeme za efektivní.

V redukci budeme potřebovat s dostatečnou přesností aproximovat diskrétní Gaussovo rozdělení na mříži. Za jakých podmínek jsme toho schopni nám shrnuje následující lemma.

Lemma 17 ([2, Proposition 2.4]). *Existuje pravděpodobnostní polynomiální algoritmus $\mathcal{A}$, který na vstupu $\mathbf{B}$ a r, kde $\mathbf{B}$ je báze n-dimenzionální mříže Λ a $r \geq \max_i \|\widetilde{\mathbf{b}}_i\| \cdot \omega(\sqrt{\log n})$, vrátí vektor z rozdělení pravděpodobnosti, které je v zanedbatelné statistické vzdálenosti od diskrétního Gaussova rozdělení $D_{\Lambda,r}$.*

Výrazem $r \geq \max_i \|\widetilde{\mathbf{b}}_i\| \cdot \omega(\sqrt{\log n})$ máme na mysli, že platí

$$r \geq \max_i \|\widetilde{\mathbf{b}}_i\| \cdot g(n),$$

kde $g(n) = \omega(\sqrt{\log n})$.

4. Redukce

V této kapitole nejprve ukážeme klasickou část Regevovy redukce [1], která redukuje problém $\mathrm{BDD}_{\Lambda,r}$ na problém search-$\mathrm{LWE}_{p,\phi}$ za předpokladu, že máme k dispozici algoritmus, který nám vrací vektory z diskrétního Gaussova rozdělení na duální mříži. Poté ukážeme Peikertovu redukci [2] $\mathrm{GapSVP}_{\zeta,\gamma}$ problému na problém search-$\mathrm{LWE}_{p,\phi}$, která využívá předchozí redukci.

Redukcí problému A na problém B myslíme algoritmus $\mathcal{A}$, který řeší problém A s přístupem k orákulu $\mathcal{O}$ řešícímu problém B. Orákulem $\mathcal{O}$ zde máme na mysli algoritmus, který řeší problém B, ale my nutně nemusíme vědět jak. Přístupem k orákulu rozumíme to, že se algoritmus $\mathcal{A}$ může dotazovat orákula $\mathcal{O}$ na instance problému B a orákulum $\mathcal{O}$ je za něj řeší. Jeden takový dotaz přitom počítáme jako jeden krok algoritmu $\mathcal{A}$. Bude-li tedy algoritmus $\mathcal{A}$ pracovat v polynomiálním čase a bude-li orákulum $\mathcal{O}$ řešit problém B také v polynomiálním čase, potom bude problém A rovněž řešitelný v polynomiálním čase. To je také důvod, proč nás takové redukce zajímají. Budeme-li totiž věřit, že problém A není řešitelný v polynomiálním čase, potom díky takové redukci můžeme věřit, že ani problém B není řešitelný v polynomiálním čase.

4.1 Regevova redukce

Začneme nejprve Regevovou redukcí. Budeme vycházet z článku [1].

Věta 18. *Nechť $\epsilon = \epsilon(n)$ je zanedbatelná funkce splňující $\epsilon < e^{-\pi}$, $p = p(n) \geq 2$ je celé a $\alpha = \alpha(n) \in (0,1)$ je reálné. Potom existuje pravděpodobnostní polynomiální algoritmus $\mathcal{A}$, který na vstupu $(\mathbf{B}, r, \mathbf{x})$, kde $\mathbf{B}$ je báze n-dimenzionální mříže Λ^*, $r \geq \sqrt{2}p\eta_\epsilon(\Lambda)$ je reálné a $\mathbf{x}$ je bod ve vzdálenosti nejvýše $\alpha p/(\sqrt{2}r)$ od mříže Λ^*, a s přístupem k*

1. *orákulu W řešícímu problém search-LWE_{p,Ψ_α} a*
2. *orákulu D, které vrací vektory z rozdělení $D_{\Lambda,r}$,*

najde jednoznačně určený vektor $\mathbf{v} \in \Lambda^*$ nejblíže k $\mathbf{x}$ s velkou pravděpodobností.

Jinými slovy, algoritmus $\mathcal{A}$ řeší problém $\mathrm{BDD}_{\Lambda^*,\alpha p/(\sqrt{2}r)}$ s velkou pravděpodobností. Podobně jako u definice LWE problému, ϵ, p a α jsou funkcemi proměnné n, která je hlavním parametrem redukce. Pravděpodobnost úspěchu i časová složitost jsou rovněž funkcemi proměnné n.

Dále nahlédneme, že takový vektor $\mathbf{v} \in \Lambda^*$ je skutečně jednoznačně určený. K tomu nám stačí ukázat, že je ve vzdálenosti ostře menší než $\lambda_1(\Lambda^*)/2$ od mříže Λ^*. Platí $\alpha p/(\sqrt{2}r) \leq \alpha/(2\eta_\epsilon(\Lambda)) < 1/(2\eta_\epsilon(\Lambda))$ z předpokladu na r a α. Zbývá ukázat, že $\eta_\epsilon(\Lambda) \geq 1/\lambda_1(\Lambda^*)$. Označme $\mathbf{m} \in \Lambda^*$ vektor takový, že $\|\mathbf{m}\| = \lambda_1(\Lambda^*)$. Potom platí

$$\rho_{\lambda_1(\Lambda^*)}(\Lambda^* \setminus \{\mathbf{0}\}) > \rho_{\lambda_1(\Lambda^*)}(\mathbf{m}) = \exp\left(-\pi\left(\frac{\|\mathbf{m}\|}{\lambda_1(\Lambda^*)}\right)^2\right) = \exp(-\pi) = e^{-\pi} > \epsilon.$$

Tedy skutečně $\eta_\epsilon(\Lambda) \geq 1/\lambda_1(\Lambda^*)$, protože $\rho_{1/r}(\Lambda^* \setminus \{\mathbf{0}\})$ roste se zmenšujícím se r.

Před samotným důkazem budeme potřebovat pomocná lemmata. První říká, že je postačující řešit problém $\mathrm{BDD}^{(p)}_{\Lambda^*,\alpha p/(\sqrt{2}r)}$ místo problému $\mathrm{BDD}_{\Lambda^*,\alpha p/(\sqrt{2}r)}$.

Lemma 19 ([1, lemma 3.5])**.** *Nechť $p \geq 2$ je celé číslo a Λ je n-dimenzionální mříž. Pak existuje efektivní algoritmus, který s přístupem k orákulu řešícímu problém $\mathrm{BDD}^{(p)}_{\Lambda,d}$, řeší problém $\mathrm{BDD}_{\Lambda,d}$.*

Důkaz. Mějme bázi $\mathbf{B}$ n-dimenzionální mříže Λ. Vstupem je $\mathbf{x} \in \mathbb{R}^n$ ve vzdálenosti nejvýše d od Λ. Chceme najít vektor mříže Λ nejblíže k bodu $\mathbf{x}$, který je jednoznačně určený. Definujme posloupnost bodů $\{\mathbf{x}_i\}_{i=1}^{n+1} \subset \mathbb{R}^n$ následovně:

- $\mathbf{x}_1 = \mathbf{x}$.
- $\mathbf{x}_{i+1} = (\mathbf{x}_i - \mathbf{B}(\mathbf{a}_i \bmod p))/p$ pro $i = 1, \ldots, n$, kde $\mathbf{a}_i = \mathbf{B}^{-1}\kappa_\Lambda(\mathbf{x}_i)$ je vektor souřadnic nejbližšího vektoru od bodu $\mathbf{x}_i$.
- Dodefinujme ještě $\mathbf{a}_{n+1} = \mathbf{B}^{-1}\kappa_\Lambda(\mathbf{x}_{n+1})$.

Protože je vektor $\mathbf{a}_i - (\mathbf{a}_i \bmod p) \in \mathbb{Z}^n$ po složkách dělitelný p, platí

$$\mathbf{v}_i = \mathbf{B}(\mathbf{a}_i - (\mathbf{a}_i \bmod p))/p \in \Lambda.$$

Podívejme se na vzdálenost $\mathbf{x}_{i+1}$ od $\mathbf{v}_i$. Platí

$$\begin{aligned}\|\mathbf{x}_{i+1} - \mathbf{v}_i\| &= \left\| \frac{\mathbf{x}_i - \mathbf{B}(\mathbf{a}_i \bmod p)}{p} - \frac{\mathbf{B}(\mathbf{a}_i - (\mathbf{a}_i \bmod p))}{p} \right\| \\ &= \frac{\|\mathbf{x}_i - \mathbf{B}\mathbf{a}_i\|}{p} = \frac{\|\mathbf{x}_i - \kappa_\Lambda(\mathbf{x}_i)\|}{p}.\end{aligned}$$

Ze zadání platí $\|\mathbf{x}_1 - \kappa_\Lambda(\mathbf{x}_1)\| \leq d$, a tedy $\|\mathbf{x}_2 - \mathbf{v}_1\| \leq d/p \leq d$. To znamená, že $\kappa_\Lambda(\mathbf{x}_2) = \mathbf{v}_1$. Induktivně můžeme pokračovat pro $i = 3, \ldots, n+1$ a dostaneme, že $\kappa_\Lambda(\mathbf{x}_i) = \mathbf{v}_{i-1}$ a $\|\mathbf{x}_i - \mathbf{v}_{i-1}\| \leq d/p^{i-1}$. Celou posloupnost umíme sestrojit, protože $(\mathbf{a}_i \bmod p)$, která na to potřebujeme, jsou výstupy orákula řešícího problém $\mathrm{BDD}^{(p)}_{\Lambda,d}$ se vstupy $\mathbf{x}_i$ (pro $i = 1, \ldots, n$).

Nyní využijeme polynomiální algoritmus na aproximaci nejbližšího vektoru popsaný v [3, Kapitola 2], který na vstupu $(\mathbf{B}', \mathbf{t})$, kde $\mathbf{B}'$ je báze n-dimenzionální mříže a $\mathbf{t} \in \mathbb{R}^n$, vrátí vektor $\mathbf{v} \in \mathcal{L}(\mathbf{B}')$ splňující

$$\|\mathbf{v} - \mathbf{t}\| \leq 2^{\frac{n}{2}+1} \cdot \mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}')).$$

Aplikujeme-li tento algoritmus na naši bázi $\mathbf{B}$ a bod $\mathbf{x}_{n+1}$, dostaneme vektor $\mathbf{w} \in \Lambda$ splňující

$$\|\mathbf{x}_{n+1} - \mathbf{w}\| \leq 2^{\frac{n}{2}+1} \cdot \mathrm{dist}(\mathbf{x}_{n+1}, \Lambda) \leq 2^{\frac{n}{2}+1} \cdot \frac{d}{p^n} \leq d$$

pro $n > 1$, protože $p \geq 2$. Pro $n = 1$ je problém triviální.

Tedy $\mathbf{w}$ je vektor mříže nejblíže k $\mathbf{x}_{n+1}$, a tedy můžeme spočítat $\mathbf{a}_{n+1}$ jako

$$\mathbf{a}_{n+1} = \mathbf{B}^{-1}\kappa_\Lambda(\mathbf{x}_{n+1}) = \mathbf{B}^{-1}\mathbf{w}.$$

Z definice $\mathbf{v}_i$ a ze vztahu $\mathbf{a}_{i+1} = \mathbf{B}^{-1}\kappa_\Lambda(\mathbf{x}_{i+1}) = \mathbf{B}^{-1}\mathbf{v}_i$ platí pro $i = 1, \ldots, n$, že

$$\mathbf{a}_{i+1} = (\mathbf{a}_i - (\mathbf{a}_i \bmod p))/p.$$

Z tohoto vztahu spočítáme

$$\mathbf{a}_n = p\mathbf{a}_{n+1} + (\mathbf{a}_n \bmod p),$$

kde $(\mathbf{a}_n \bmod p)$ jsme obdrželi z orákula při sestrojování posloupnosti $\{\mathbf{x}_i\}_{i=1}^{n+1}$. Stejným procesem dopočítáme $\mathbf{a}_{n-1}, \ldots, \mathbf{a}_1$. Protože platí, že $\mathbf{a}_1 = \mathbf{B}^{-1}\kappa_\Lambda(\mathbf{x}_1)$, dostáváme

$$\kappa_\Lambda(\mathbf{x}) = \kappa_\Lambda(\mathbf{x}_1) = \mathbf{B}\mathbf{a}_1,$$

čímž jsme našli hledaný nejbližší vektor. Algoritmus očividně pracuje v polynomiálním čase. Tím je důkaz hotov. □

Bude-li orákulum řešící problém $\mathrm{BDD}^{(p)}_{\Lambda,d}$ vracet souřadnice modulo p nejbližšího vektoru s velkou pravděpodobností, potom bude výše popsaný algoritmus vracet nejbližší vektor rovněž s velkou pravděpodobností, protože jednotlivé pokusy jsou nezávislé a platí [9], že

$$(1 - \mathrm{negl}(n))^{\mathrm{poly}(n)} = 1 - \mathrm{negl}(n). \tag{4.1}$$

Stejný argument použijeme později i v důkazu věty 22. V redukci budeme potřebovat řešit search-$\mathrm{LWE}_{p,\phi}$ pro $\phi = \Psi_\beta$, kde $\beta \leq \alpha$ může být neznámá. Bez důkazu uvedeme lemma, které říká, že toho jsme schopni.

Lemma 20 ([1, Lemma 3.7])**.** *Buď $p = p(n) \geq 2$ celé a buď $\alpha = \alpha(n) \in (0,1)$ reálné. Potom existuje pravděpodobnostní polynomiální algoritmus, který s přístupem k orákulu W řešícímu search-$\mathrm{LWE}_{p,\phi}$ problém pro $\phi = \Psi_\alpha$, řeší search-$\mathrm{LWE}_{p,\phi}$ problém pro $\phi = \Psi_\beta$, kde $\beta \leq \alpha$, aniž by znal hodnotu β.*

Pro samotný důkaz Regevovy redukce budeme potřebovat ještě následující technické lemma, které se týká Gaussových rozdělení v souvislosti s mřížemi.

Lemma 21 ([1, Corollary 3.10])**.** *Nechť Λ je n-dimenzionální mříž, $\mathbf{z}, \mathbf{u} \in \mathbb{R}^n$ jsou vektory a $r, \alpha > 0$ jsou reálná. Předpokládejme dále, že*

$$1/\sqrt{1/r^2 + (\|\mathbf{z}\|/\alpha)^2} \geq \eta_\epsilon(\Lambda)$$

pro $\epsilon < \frac{1}{2}$. Potom platí, že

$$\Delta(X, D_\beta) \leq 2\epsilon,$$

kde $X = \langle \mathbf{z}, D_{\Lambda+\mathbf{u},r} \rangle + D_\alpha$ a $\beta = \sqrt{(r\|\mathbf{z}\|)^2 + \alpha^2}$.

Speciálně platí, že rozdělení $X \bmod 1$ je ve statistické vzdálenosti nejvýše 2ϵ od rozdělení $D_\beta \bmod 1 = \Psi_\beta$, protože statistická vzdálenost se nemůže zvětšit aplikováním funkce, v našem případě funkce modulo 1. Nyní již máme vše připraveno na to, abychom mohli ukázat důkaz redukce ze začátku této sekce.

Důkaz věty 18. Díky lemmatu 19 stačí ukázat, že algoritmus $\mathcal{A}$ řeší problém $\mathrm{BDD}^{(p)}_{\Lambda^*,\alpha p/(\sqrt{2}r)}$. Zároveň můžeme z lemmatu 20 předpokládat, že $\mathcal{A}$ má přístup také k orákulu W' řešícímu problém search-$\mathrm{LWE}_{p,\Psi_\beta}$ pro $\beta \leq \alpha$, kde β může být i neznámá. Označme n^c počet dvojic, které potřebuje W' na řešení problému search-$\mathrm{LWE}_{p,\Psi_\beta}$. Nyní popíšeme algoritmus $\mathcal{A}$. Na vstupu je bod $\mathbf{x} \in \mathbb{R}^n$ ve vzdálenosti nejvýše $\alpha p/(\sqrt{2}r)$ od mříže Λ^* a úkolem je najít souřadnice modulo p

nejbližšího vektoru $\mathbf{w} \in \Lambda^*$ od bodu $\mathbf{x}$. Algoritmus $\mathcal{A}$ použije proceduru $\mathcal{P}$, která (na vstupu toto $\mathbf{x}$) vrátí dvojici z rozdělení pravděpodobnosti blízkého $A_{\mathbf{s},\Psi_\beta}$, kde $\mathbf{s} = \mathbf{B}^\top \kappa_{\Lambda^*}(\mathbf{x}) \bmod p$ a $\beta \leq \alpha$. Toto $\mathbf{s}$ je řešením problému $\mathrm{BDD}^{(p)}_{\Lambda^*,\alpha p/(\sqrt{2}r)}$, protože $(\mathbf{B}^{-1})^\top$ je báze Λ^* a $((\mathbf{B}^{-1})^\top)^{-1} = \mathbf{B}^\top$. Algoritmus $\mathcal{A}$ použije proceduru $\mathcal{P}$ n^c-krát a s velkou pravděpodobností najde hledané $\mathbf{s}$ pomocí orákula W'.

Nyní popíšeme proceduru $\mathcal{P}$ a analyzujeme chybu aproximace pomocí statistické vzdálenosti. Výstupem procedury $\mathcal{P}$ je dvojice

$$(\mathbf{a}, \langle \mathbf{x}, \mathbf{v} \rangle / p + e \bmod 1) \in \mathbb{Z}_p^n \times \mathbb{T},$$

kde

- $\mathbf{v} \leftarrow D_{\Lambda,r}$,
- $\mathbf{a} = \mathbf{B}^{-1}\mathbf{v} \bmod p$,
- $e \leftarrow D_{\alpha/\sqrt{2}}$.

Chceme ukázat, že takto vytvořené rozdělení pravděpodobnosti, které si označíme $\mathcal{D}$, je v zanedbatelné statistické vzdálenosti od rozdělení $A_{\mathbf{s},\Psi_\beta}$ pro nějaké $\beta \leq \alpha$.

Nejprve potřebujeme ukázat, že rozdělení první složky $\mathbf{a}$, které si označíme $\mathcal{D}_1$, je v zanedbatelné statistické vzdálenosti od rovnoměrného rozdělení na $\mathbb{Z}_p^n$. Podíváme se, jaká je pravděpodobnost, že obdržíme nějaké $\mathbf{a} \in \mathbb{Z}_p^n$. Platí

$$\Pr[\mathcal{D}_1 = \mathbf{a}] = \frac{\rho_r(p\Lambda + \mathbf{Ba})}{\rho_r(\Lambda)},$$

protože $\mathbf{B}^{-1}(p\Lambda + \mathbf{Ba}) \bmod p = (p\mathbb{Z}^n + \mathbf{a}) \bmod p = \mathbf{a}$. Z lemmatu 8 a předpokladu na r plyne, že $\eta_\epsilon(p\Lambda) = p\eta_\epsilon(\Lambda) < r$. Z lemmatu 10 dostaneme, že

$$\rho_r(p\Lambda + \mathbf{Ba}) \in (1 \pm \epsilon) \cdot r^n \det(\Lambda^*/p),$$

a tedy

$$\begin{aligned} \Pr[\mathcal{D}_1 = \mathbf{a}] = \frac{\rho_r(p\Lambda + \mathbf{Ba})}{\rho_r(\Lambda)} &\in (1 \pm \epsilon) \cdot \frac{r^n \det(\Lambda^*/p)}{\rho_r(\Lambda)} \\ &= (1 \pm \epsilon) \cdot K, \end{aligned} \tag{4.2}$$

kde jsme označili

$$K = \frac{r^n \det(\Lambda^*/p)}{\rho_r(\Lambda)},$$

které nezávisí na $\mathbf{a}$. Protože platí

$$\sum_{\mathbf{a} \in \mathbb{Z}_p^n} \Pr[\mathcal{D}_1 = \mathbf{a}] = 1,$$

dostaneme, že

$$(1 - \epsilon) \cdot K \leq \frac{1}{p^n} \leq (1 + \epsilon) \cdot K.$$

Použitím vztahu 4.2 dále dostaneme, že

$$\frac{1 - \epsilon}{1 + \epsilon} \cdot \frac{1}{p^n} \leq \Pr[\mathcal{D}_1 = \mathbf{a}] \leq \frac{1 + \epsilon}{1 - \epsilon} \cdot \frac{1}{p^n}.$$

Všimněme si, že výsledný odhad na pravděpodobnost nezávisí na $\mathbf{a}$. Dále platí, že

$$\Pr[\mathcal{U}(\mathbb{Z}_p^n) = \mathbf{a}] = \frac{1}{p^n},$$

a tedy

$$\left|\Pr[\mathcal{D}_1 = \mathbf{a}] - \Pr[\mathcal{U}(\mathbb{Z}_p^n) = \mathbf{a}]\right| \leq \frac{1}{p^n} \cdot \frac{2\epsilon}{1-\epsilon}.$$

Pro statistickou vzdálenost tedy máme, že

$$\begin{aligned}\Delta(\mathcal{D}_1, \mathcal{U}(\mathbb{Z}_p^n)) &= \frac{1}{2} \sum_{\mathbf{a} \in \mathbb{Z}_p^n} \left|\Pr[\mathcal{D}_1 = \mathbf{a}] - \Pr[\mathcal{U}(\mathbb{Z}_p^n) = \mathbf{a}]\right| \\ &\leq \frac{1}{2} \sum_{\mathbf{a} \in \mathbb{Z}_p^n} \frac{1}{p^n} \cdot \frac{2\epsilon}{1-\epsilon} = \frac{\epsilon}{1-\epsilon} < 2\epsilon,\end{aligned}$$

což nám stačí, protože ϵ je zanedbatelná funkce.

Protože se v rozdělení $A_{\mathbf{s},\Psi_\beta}$ nejprve volí $\mathbf{a}' \leftarrow \mathcal{U}(\mathbb{Z}_p^n)$ a druhá složka poté závisí na tomto $\mathbf{a}'$, zajímá nás u procedury $\mathcal{P}$ rozdělení druhé složky $\langle \mathbf{x}, \mathbf{v} \rangle / p + e \bmod 1$ podmíněné na konkrétní hodnotu $\mathbf{a}$. Takto podmíněné rozdělení si označíme $\mathcal{D}_{2,\mathbf{a}}$. Označme si dále $\mathbf{x}' = \mathbf{x} - \kappa_{\Lambda^*}(\mathbf{x})$, tedy $\mathbf{x} = \mathbf{x}' + \kappa_{\Lambda^*}(\mathbf{x})$. Z předpokladu na vzdálenost bodu $\mathbf{x}$ od mříže Λ^* plyne, že $\|\mathbf{x}'\| \leq \alpha p / (\sqrt{2} r)$, neboli $\sqrt{2}\|\mathbf{x}'\| / (\alpha p) \leq 1/r$. Dále platí

$$\begin{aligned}\langle \mathbf{x}, \mathbf{v} \rangle / p + e \bmod 1 &= \langle \mathbf{x}'/p, \mathbf{v} \rangle + e + \langle \kappa_{\Lambda^*}(\mathbf{x}), \mathbf{v} \rangle / p \bmod 1 \\ &= (\langle \mathbf{x}'/p, \mathbf{v} \rangle + e \bmod 1) + (\langle \kappa_{\Lambda^*}(\mathbf{x}), \mathbf{v} \rangle / p \bmod 1) \bmod 1.\end{aligned}$$

Připomeňme, že pro $\mathbf{u}, \mathbf{w} \in \mathbb{R}^n$ a $\mathbf{A} \in \mathbb{R}^{n \times n}$ regulární platí, že

$$\langle \mathbf{A}^{-1}\mathbf{u}, \mathbf{A}^\top \mathbf{w} \rangle = (\mathbf{A}^{-1}\mathbf{u})^\top \mathbf{A}^\top \mathbf{w} = \mathbf{u}^\top (\mathbf{A}^{-1})^\top \mathbf{A}^\top \mathbf{w} = \mathbf{u}^\top \mathbf{w} = \langle \mathbf{u}, \mathbf{w} \rangle.$$

Pro volbu $\mathbf{A} = \mathbf{B}^*$ a ze vztahu $(\mathbf{B}^*)^\top = \mathbf{B}^{-1}$ dostaneme, že

$$\langle \kappa_{\Lambda^*}(\mathbf{x}), \mathbf{v} \rangle = \langle (\mathbf{B}^*)^{-1} \kappa_{\Lambda^*}(\mathbf{x}), \mathbf{B}^{-1}\mathbf{v} \rangle.$$

Protože $(\mathbf{B}^*)^{-1}\kappa_{\Lambda^*}(\mathbf{x})$ jsou souřadnice vektoru $\kappa_{\Lambda^*}(\mathbf{x}) \in \Lambda^*$ vůči bázi $\mathbf{B}^*$ mříže Λ^*, platí $(\mathbf{B}^*)^{-1}\kappa_{\Lambda^*}(\mathbf{x}) \in \mathbb{Z}^n$. Podobně pro $\mathbf{B}^{-1}\mathbf{v}$. Tedy

$$\langle \kappa_{\Lambda^*}(\mathbf{x}), \mathbf{v} \rangle = \langle (\mathbf{B}^*)^{-1} \kappa_{\Lambda^*}(\mathbf{x}), \mathbf{B}^{-1}\mathbf{v} \rangle \in \mathbb{Z},$$

a proto

$$\begin{aligned}\langle \kappa_{\Lambda^*}(\mathbf{x}), \mathbf{v} \rangle \bmod p &= \langle (\mathbf{B}^*)^{-1} \kappa_{\Lambda^*}(\mathbf{x}), \mathbf{B}^{-1}\mathbf{v} \rangle \bmod p \\ &= \langle (\mathbf{B}^*)^{-1} \kappa_{\Lambda^*}(\mathbf{x}) \bmod p, \mathbf{B}^{-1}\mathbf{v} \bmod p \rangle \bmod p \\ &= \langle \mathbf{s}, \mathbf{a} \rangle \bmod p,\end{aligned}$$

neboli

$$\langle \kappa_{\Lambda^*}(\mathbf{x}), \mathbf{v} \rangle / p \bmod 1 = \langle \mathbf{s}, \mathbf{a} \rangle / p \bmod 1.$$

Nyní se podíváme na zbývající část druhé složky, tedy na $\langle \mathbf{x}'/p, \mathbf{v} \rangle + e \bmod 1$. Rozdělení e známe, $\mathbf{x}'/p$ je fixní, takže zbývá zjistit rozdělení vektoru $\mathbf{v}$. Připomeňme, že podmiňujeme na nějakou konkrétní hodnotu $\mathbf{a}$. Podobnou úvahou jako

výše dostaneme, že rozdělení vektoru $\mathbf{v}$ je právě $D_{p\Lambda+\mathbf{Ba},r}$. Zbývající část druhé složky $\mathcal{D}_{2,\mathbf{a}}$ je tedy skalární součin fixního vektoru a náhodného vektoru s diskrétním Gaussovým rozdělením na mříži zašumělý hodnotou z rozdělení $D_{\alpha/\sqrt{2}}$. Pokusíme se tedy použít lemma 21. Potřebujeme ověřit předpoklady. Platí

$$\frac{1}{\sqrt{1/r^2 + (\sqrt{2}\|\mathbf{x}'\|/(\alpha p))^2}} \geq \frac{1}{\sqrt{1/r^2 + 1/r^2}} = \frac{r}{\sqrt{2}} \geq p\eta_\epsilon(\Lambda) = \eta_\epsilon(p\Lambda).$$

Tedy platí předpoklady lemmatu 21 a rozdělení $\langle \mathbf{x}'/p, \mathbf{v}\rangle + e$ je ve statistické vzdálenosti nejvýše 2ϵ od D_β pro

$$\beta = \sqrt{(r\|\mathbf{x}'\|/p)^2 + \alpha^2/2} \leq \sqrt{\alpha^2/2 + \alpha^2/2} = \alpha.$$

Z poznámky pod lemmatem tedy plyne, že rozdělení $\langle \mathbf{x}'/p, \mathbf{v}\rangle + e \bmod 1$ je ve statistické vzdálenosti nejvýše 2ϵ od rozdělení Ψ_β. Dohromady tedy dostaneme, že rozdělení $\mathcal{D}_{2,\mathbf{a}}$ je ve statistické vzdálenosti nejvýše 2ϵ od rozdělení X, kde

$$X = \langle \mathbf{s}, \mathbf{a}\rangle/p + f \bmod 1$$

pro $f \leftarrow \Psi_\beta$. Jak vidíme, rozdělení X je přesně druhá složka rozdělení $A_{\mathbf{s},\Psi_\beta}$ podmíněná na hodnotu $\mathbf{a}$.

Z lemmatu 14 plyne, že $\Delta(\mathcal{D},A_{\mathbf{s},\Psi_\beta}) \leq 2 \cdot 2\epsilon + 2\epsilon = 6\epsilon$. Protože používáme $n^c = \text{poly}(n)$ dvojic, bude jejich celkové rozdělení stále v zanedbatelné statistické vzdálenosti od rozdělení n^c dvojic z $A_{\mathbf{s},\Psi_\beta}$, jak již bylo zmíněno v sekci o statistické vzdálenosti. Tedy orákulum W' vrátí $\mathbf{s}$ s pravděpodobností

$$\Pr[W' = \mathbf{s}] \geq 1 - \text{negl}(n) - \text{negl}(n) = 1 - \text{negl}(n),$$

čímž je důkaz hotov. □

Tím jsme dokázali klasickou část Regevovy redukce. Tu nyní využijeme k redukci problému $\text{GapSVP}_{\zeta,\gamma}$ na problém $\text{search-LWE}_{p,\Psi_\alpha}$, kterou ve svém článku publikoval Chris Peikert [2].

4.2 Peikertova redukce

Nyní ukážeme Peikertovu redukci. Budeme vycházet z článku [2].

Věta 22. *Nechť $\alpha = \alpha(n) \in (0,1)$ a $\gamma = \gamma(n) \geq n/(\alpha\sqrt{\log n})$ jsou reálná. Dále buď $\zeta = \zeta(n) \geq \gamma(n)$ reálné a $p = p(n) \geq (\zeta/\sqrt{n}) \cdot \omega(\sqrt{\log n})$ celé. Potom existuje pravděpodobnostní polynomiální algoritmus $\mathcal{A}$, který s přístupem k orákulu W řešícímu problém $\text{search-LWE}_{p,\Psi_\alpha}$, řeší problém $\text{GapSVP}_{\zeta,\gamma}$ s velkou pravděpodobností.*

Podobně jako u Regevovy redukce, n je hlavním parametrem redukce a ostatní parametry, časová složitost a pravděpodobnost úspěchu jsou funkcemi n. Podobně jako v lemmatu 17, výrazem $p \geq (\zeta/\sqrt{n}) \cdot \omega(\sqrt{\log n})$ značíme to, že $p \geq (\zeta/\sqrt{n}) \cdot g(n)$, kde $g(n) = \omega(\sqrt{\log n})$. Pokud by platilo $\zeta(n) = 2^{n/2}$, dostali bychom redukci standardního problému GapSVP_γ. Platí $\sqrt{n} = \omega(\sqrt{\log n})$, a tedy volbou $g(n) = \sqrt{n}$ dostaneme, že pro $p \geq 2^{n/2}$ platí $p \geq (\zeta/\sqrt{n}) \cdot \omega(\sqrt{\log n})$. Tedy pro $p \geq 2^{n/2}$ dostaneme redukci standardního problému GapSVP_γ.

Důkaz věty 22. Redukce se skládá ze dvou částí. První redukuje problém $\mathrm{BDD}_{\Lambda,r}$ na problém search-$\mathrm{LWE}_{p,\Psi_\alpha}$. Tuto část máme k dispozici z předchozí sekce, příslušný algoritmus bude hrát nyní roli orákula a budeme ho značit R. Pouze si dejme pozor, že nyní budeme potřebovat hledat nejbližší vektor v mříži Λ, kdežto v Regevově redukci jsme ho hledali v mříži Λ^*. To ale nevadí, protože platí $(\Lambda^*)^* = \Lambda$, tedy pouze vyměníme role mříží Λ a Λ^*. Druhá část redukuje problém $\mathrm{GapSVP}_{\zeta,\gamma}$ na problém $\mathrm{BDD}_{\Lambda,r}$. Spojením těchto dvou částí dostaneme redukci problému $\mathrm{GapSVP}_{\zeta,\gamma}$ na problém search-$\mathrm{LWE}_{p,\Psi_\alpha}$.

Na vstupu tedy dostaneme dvojici $(\mathbf{B}, d)$, kde $d > 0$ je reálné a $\mathbf{B}$ je báze n-dimenzionální mříže Λ splňující $\min_i \|\widetilde{\mathbf{b}}_i\| \geq 1, \lambda_1(\Lambda) \leq \zeta$ a $1 \leq d \leq \zeta/\gamma$. Naším úkolem je rozhodnout, zda $\lambda_1(\Lambda) \leq d$ nebo $\lambda_1(\Lambda) > \gamma \cdot d$. Chování orákula R řešícího problém $\mathrm{BDD}_{\Lambda,r}$ nám pomůže rozhodnout, která situace nastala. V redukci zvolíme bod $\mathbf{x}$ v jisté vzdálenosti od nějakého vektoru mříže $\mathbf{u} \in \Lambda$. Pokud bude platit $\lambda_1(\Lambda) \leq d$, potom bude vektor $\mathbf{u}$ nejbližší vektor mříže k bodu $\mathbf{x}$ a orákulum R nám vrátí vektor $\mathbf{u}$ s velkou pravděpodobností. Naopak pokud bude platit $\lambda_1(\Lambda) > \gamma \cdot d$, potom bude pravděpodobnost, že orákulum R vrátí vektor $\mathbf{u}$, nejvýše $1 - 1/\mathrm{poly}(n)$. Tento proces zopakujeme N-krát, kde $N = \mathrm{poly}(n)$ je dostatečně velké v porovnání s pravděpodobností z předchozí věty. Pokud v každém pokusu vrátí orákulum R vektor $\mathbf{u}$, prohlásíme, že $\lambda_1(\Lambda) \leq d$. Pokud alespoň jednou toto orákulum vrátí jiný vektor než $\mathbf{u}$, prohlásíme, že $\lambda_1(\Lambda) > \gamma \cdot d$.

Nyní detailně popíšeme a analyzujeme výše zmíněný proces:

1. Algoritmus $\mathcal{A}$ zvolí vektor $\mathbf{w}$ rovnoměrně náhodně z otevřené koule $d' \cdot \mathcal{B}_n$, kde $d' = d \cdot \sqrt{n/(4 \log n)}$. Tedy $\mathbf{w} \leftarrow \mathcal{U}(d' \cdot \mathcal{B}_n)$. Označme $\mathbf{x} = \mathbf{w} \bmod \mathbf{B}$ a $\mathbf{u} = \mathbf{x} - \mathbf{w}$. Platí $\mathbf{u} \in \Lambda$.

2. Algoritmus $\mathcal{A}$ zavolá orákulum R se vstupem $(\mathbf{B}, r, \mathbf{x})$, kde

$$r = \frac{p \cdot \sqrt{2n}}{\gamma \cdot d}.$$

Označme $\mathbf{v}$ vektor, který nám vrátí orákulum R.

Nejprve musíme ověřit, že vůbec máme orákulum R k dispozici. Jinými slovy, potřebujeme ověřit předpoklady věty 18. Orákulum W, které je schopné řešit problém search-$\mathrm{LWE}_{p,\Psi_\alpha}$, máme k dispozici z předpokladu věty. Za orákulum D vracející vektory z rozdělení $D_{\Lambda^*,r}$ vezmeme algoritmus z lemmatu 17, což můžeme, protože vrací vektory z rozdělení v zanedbatelné statistické vzdálenosti od rozdělení $D_{\Lambda^*,r}$. Formálně bychom totiž mohli použít stejné argumenty jako v důkazu věty 18. Ověříme tedy předpoklady lemmatu 17. Protože $\mathbf{B}$ je báze mříže Λ, je $\mathbf{D} = \mathbf{B}^*$ báze mříže Λ^*. Z lemmatu 3 plyne, že $\max_i \|\widetilde{\mathbf{d}}_i\| = 1/\min_i \|\widetilde{\mathbf{b}}_i\|$, a tedy $\max_i \|\widetilde{\mathbf{d}}_i\| \leq 1$ z předpokladu na bázi $\mathbf{B}$. Dále platí

$$r = \frac{p \cdot \sqrt{2n}}{\gamma \cdot d} \geq \frac{p \cdot \sqrt{2n}}{\zeta} \geq \omega(\sqrt{\log n}) \geq \max_i \|\widetilde{\mathbf{d}}_i\| \cdot \omega(\sqrt{\log n}),$$

kde první nerovnost plyne z předpokladu na d z definice $\mathrm{GapSVP}_{\zeta,\gamma}$ problému, druhá z dolního odhadu na p z předpokladu věty a třetí z odhadu, který jsme odvodili výše. Tedy můžeme použít algoritmus z lemmatu 17 se vstupem $(\mathbf{D}, r)$,

abychom mohli aproximovat rozdělení $D_{\Lambda^*,r}$.

Nyní rozlišíme dva případy. Nejprve předpokládejme, že $\lambda_1(\Lambda) > \gamma \cdot d$. Poté platí

$$r = \frac{p \cdot \sqrt{2n}}{\gamma \cdot d} > \frac{p \cdot \sqrt{2n}}{\lambda_1(\Lambda)} \geq \sqrt{2}p \cdot \eta_\epsilon(\Lambda^*)$$

pro $\epsilon(n) = 2^{-n} = \text{negl(n)}$, kde první nerovnost plyne z našeho současného předpokladu na $\lambda_1(\Lambda)$ a druhá z lemmatu 9. Tedy r je dostatečně velké pro orákulum R, aby našlo nejbližší vektor s velkou pravděpodobností. Protože $\mathbf{x} - \mathbf{w} \in \Lambda$, platí $\text{dist}(\Lambda, \mathbf{x}) \leq \|\mathbf{w}\|$. Nyní odhadneme tuto normu. Z předpokladu věty platí

$$\frac{n}{\alpha\sqrt{\log n}} \leq \gamma,$$

a tedy

$$\sqrt{\frac{n}{\log n}} \leq \frac{\gamma \cdot \alpha}{\sqrt{n}}. \tag{4.3}$$

Z nerovnosti (4.3) a z definice $\mathbf{w}$ a r dostáváme

$$\|\mathbf{w}\| < d' = d \cdot \sqrt{\frac{n}{4\log n}} \leq \frac{\gamma \cdot \alpha \cdot d}{2\sqrt{n}} = \frac{\alpha p}{\sqrt{2}r}.$$

Vzdálenost vektoru $\mathbf{x}$ od mříže Λ je tedy dostatečně malá pro orákulum R. Zároveň platí

$$\lambda_1(\Lambda) > \gamma \cdot d \geq \frac{d \cdot n}{\alpha\sqrt{\log n}} > \frac{d \cdot n}{\sqrt{\log n}} = 2d'\sqrt{n} \geq 2d',$$

kde první nerovnost plyne z našeho současného předpokladu na $\lambda_1(\Lambda)$, druhá a třetí z odhadu na γ a α z předpokladu věty. To znamená, že

$$\text{dist}(\mathbf{x}, \mathbf{u}) = \|\mathbf{w}\| < d' < \frac{\lambda_1(\Lambda)}{2},$$

neboli $\mathbf{u} \in \Lambda$ je nejbližší vektor mříže k bodu $\mathbf{x}$ a tedy $\mathbf{v} = \mathbf{u}$ s velkou pravděpodobností. Zopakujeme-li tento proces N-krát, kde $N = \text{poly}(n)$, potom ze vztahu 4.1 víme, že pravděpodobnost, že pokaždé dostaneme $\mathbf{v} = \mathbf{u}$, bude stále velká.

Nyní předpokládejme, že $\lambda_1(\Lambda) \leq d$. Buď $\mathbf{z} \in \Lambda$ vektor splňující $\|\mathbf{z}\| = \lambda_1(\Lambda)$. Uvažujme nyní experiment, kdy místo $\mathbf{w}$ vezmeme $\mathbf{w}' = \mathbf{w} + \mathbf{z}$, kde $\mathbf{w} \leftarrow \mathcal{U}(d' \cdot \mathcal{B}_n)$, a orákulum R zavoláme se vstupem $(\mathbf{B}, r, \mathbf{x}')$, kde $\mathbf{x}' = \mathbf{w}' \bmod \mathbf{B}$. Statistická vzdálenost rozdělení vektorů $\mathbf{w}$ a $\mathbf{w}'$ je z lemmatu 16 menší než $1 - 1/\text{poly}(n)$ a z poznámky pod lemmatem 15 se nemůže zvětšit aplikováním orákula R. Tedy speciálně platí, že

$$\Pr[R(\mathbf{x}) = \mathbf{x} - \mathbf{w}] - \Pr[R(\mathbf{x}') = \mathbf{x}' - \mathbf{w}'] \leq 1 - \frac{1}{\text{poly}(n)}.$$

Dále platí, že

$$\Pr[R(\mathbf{x}') = \mathbf{x}' - \mathbf{w}'] + \Pr[R(\mathbf{x}') = \mathbf{x}' - \mathbf{w}] \leq 1,$$

protože $\mathbf{w} \neq \mathbf{w}'$ a tedy jsou jevy $R(\mathbf{x}') = \mathbf{x}' - \mathbf{w}'$, $R(\mathbf{x}') = \mathbf{x}' - \mathbf{w}$ disjunktní. Dohromady dostáváme, že

$$\Pr[R(\mathbf{x}) = \mathbf{x} - \mathbf{w}] \leq 2 - \frac{1}{\text{poly}(n)} - \Pr[R(\mathbf{x}') = \mathbf{x}' - \mathbf{w}].$$

Nyní si všimneme, že $\mathbf{x}' = \mathbf{z} + \mathbf{w} \bmod \mathbf{B} = \mathbf{w} \bmod \mathbf{B}$, protože $\mathbf{z} \in \Lambda$, a tedy rozdělení bodů $\mathbf{x}$ a $\mathbf{x}'$ jsou totožná. To znamená, že

$$\Pr[R(\mathbf{x}') = \mathbf{x}' - \mathbf{w}] = \Pr[R(\mathbf{x}) = \mathbf{x} - \mathbf{w}],$$

a tedy po nahrazení

$$\Pr[R(\mathbf{x}) = \mathbf{x} - \mathbf{w}] \leq 1 - \frac{1}{2 \cdot \text{poly}(n)} = 1 - \frac{1}{\text{poly}(n)}.$$

Z poznámky pod lemmatem 16 víme, že bude-li $N = \text{poly}(n)$ dostatečně velké, je velká pravděpodobnost, že při N pokusech bude alespoň jednou platit $\mathbf{v} \neq \mathbf{u}$. Tím je důkaz hotov. □

Poznamenejme, že N z předchozího důkazu nepotřebujeme znát. Věta totiž pouze tvrdí, že existuje algoritmus $\mathcal{A}$, který řeší problém $\text{GapSVP}_{\zeta,\gamma}$. To, že nevíme, kolikrát přesně má $\mathcal{A}$ zopakovat výše zmíněný proces, tedy nevadí. Důležité je, že nějaké N splňující naše požadavky existuje.

5. Schéma na výměnu klíče

5.1 Popis schématu

V této části ukážeme jedno z možných využití problému LWE. Popíšeme schéma na výměnu klíče, jehož bezpečnost je založena právě na tomto problému. Budeme vycházet z článků [10, 11]. Schématem na výměnu klíče máme na mysli metodu, jak se dvě strany mohou dohodnout na společném tajném klíči, který zůstane tajným i pro útočníka, který zná informace, které si obě strany vyměnily během vzájemné komunikace. Pro jednoduchost popíšeme variantu, kde má výsledný klíč pouze jeden bit. Idea je založena na následující identitě

$$\mathbf{x}^\top(\mathbf{M}^\top\mathbf{y}) = (\mathbf{M}\mathbf{x})^\top\mathbf{y} \mod p,$$

kde $\mathbf{M} \in \mathbb{Z}_p^{n\times n}$ a $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_p^n$. Představme si následující situaci. Vektory $\mathbf{x}, \mathbf{y}$ budou postupně tajné informace komunikujících stran A, B a matice $\mathbf{M}$ veřejný parametr. Strany si vymění součiny $\mathbf{M}^\top\mathbf{y}$ a $\mathbf{M}\mathbf{x}$ a společným klíčem bude $\mathbf{x}^\top\mathbf{M}^\top\mathbf{y}$, což si obě strany mohou lehce dopočítat ze své tajné informace a z toho, co obdrží od druhé strany. Takové schéma by ale očividně nebylo bezpečné. Útočník by ze součinů $\mathbf{M}^\top\mathbf{y}$ a $\mathbf{M}\mathbf{x}$ lehce dopočítal $\mathbf{x}$ a $\mathbf{y}$ a tím i výsledný klíč. Co tedy tyto součiny trochu pozměnit, aby bylo těžké dopočítat $\mathbf{x}$ a $\mathbf{y}$. Nebo lépe, aby součiny vypadaly pseudonáhodně. To nás přirozeně přivádí na problém LWE. Jak jsme již zmínili, budeme využívat verzi HNF-decision-LWE$_{p,\chi}$. V následující části uvidíme proč. Pozměníme tedy předchozí proces tak, že nyní:

- Matice $\mathbf{M} \in \mathbb{Z}_p^n$ zůstává veřejným parametrem, $\chi = \lfloor D_{\alpha p} \rceil \bmod p$ je chybové rozdělení na $\mathbb{Z}_p$.
- Strana A zvolí $\mathbf{x}, \mathbf{e}_A \leftarrow \chi^n$ a spočítá $\mathbf{p}_A = \mathbf{M}\mathbf{x} + \mathbf{e}_A \bmod p$, které pošle straně B.
- Strana B zvolí $\mathbf{y}, \mathbf{e}_B \leftarrow \chi^n$ a spočítá $\mathbf{p}_B = \mathbf{M}^\top\mathbf{y}+\mathbf{e}_B \bmod p$, které pošle zpět straně A. Kromě toho spočítá $K_B = \mathbf{p}_A^\top\mathbf{y} \bmod p = \mathbf{x}^\top\mathbf{M}^\top\mathbf{y} + \mathbf{e}_A^\top\mathbf{y} \bmod p$.
- Strana A spočítá $K_A = \mathbf{x}^\top\mathbf{p}_B \bmod p = \mathbf{x}^\top\mathbf{M}^\top\mathbf{y} + \mathbf{x}^\top\mathbf{e}_B \bmod p$.

Podle prvního návrhu by nyní společným klíčem mělo být K_A, respektive K_B. To ale bohužel fungovat nebude, protože kvůli přidaným chybovým vektorům obecně $K_A \neq K_B$. Ale jak si můžeme všimnout, K_A se zčásti podobá K_B. Platí

$$\begin{aligned} K_A - K_B \bmod p &= \mathbf{x}^\top\mathbf{M}^\top\mathbf{y} + \mathbf{x}^\top\mathbf{e}_B - \mathbf{x}^\top\mathbf{M}^\top\mathbf{y} - \mathbf{e}_A^\top\mathbf{y} \bmod p \\ &= \mathbf{x}^\top\mathbf{e}_B - \mathbf{e}_A^\top\mathbf{y} \bmod p. \end{aligned}$$

Vektory $\mathbf{x}, \mathbf{y}, \mathbf{e}_A, \mathbf{e}_B$ pochází ze zaokrouhleného Gaussova rozdělení, tedy jednotlivé složky vektorů budou koncentrovány kolem nuly. To znamená, že i rozdíl $K_A - K_B$ bude blízko nuly. To je důvod, proč používáme HNF-decision-LWE$_{p,\chi}$ problém. Abychom mohli smysluplně používat výraz blízko nuly, budeme uvažovat prvky $\mathbb{Z}_p$ z množiny $(-\frac{p}{2}, \frac{p}{2}] \cap \mathbb{Z}$.

Platí $K_A, K_B \in \mathbb{Z}_p$, ale my jsme zmínili, že výsledný klíč bude mít pouze jeden bit. Využijeme tedy toho, že K_A, K_B jsou blízko sebe a strany A, B z těchto dvou

blízkých hodnot odvodí výsledný bit tak, aby pro útočníka vypadal náhodně. K tomuto účelu strana B nejprve spočítá K_B novým způsobem jako

$$K_B = \mathbf{p}_A^\top \mathbf{y} + e,$$

kde $e \leftarrow \chi$. Potom spočítá nový společný klíč $K = f(K_B)$, kde $f : \mathbb{Z}_p \to \mathbb{Z}_2$. Dále spočítá indicii $c = g(K_B)$, kde $g : \mathbb{Z}_p \to \mathbb{Z}_2$. Tu pošle zpět straně A společně s $\mathbf{p}_B$, která z nich spočítá společný klíč K jako $K = \mathrm{rec}(K_A, c)$, kde $\mathrm{rec} : \mathbb{Z}_p \times \mathbb{Z}_2 \to \mathbb{Z}_2$. Protože indicie c je součástí komunikace mezi A a B, a je tedy dostupná potenciálnímu útočníkovi, požadujeme, aby funkce f, g splňovaly

$$\Pr[f(x) = 0 \mid g(x) = 0] = \Pr[f(x) = 0 \mid g(x) = 1] = \frac{1}{2} \tag{5.1}$$

pro $x \leftarrow \mathcal{U}(\mathbb{Z}_p)$. Bude-li tedy K_B pro útočníka vypadat náhodně, potom mu samotná znalost c nedá žádnou informaci o klíči K. Dalším přirozeným požadavkem je, aby pro K_A, K_B platilo $\mathrm{rec}(K_A, g(K_B)) = f(K_B)$, neboli, aby obě strany skutečně obdržely stejný klíč. To bude ovšem záviset na vzdálenosti K_A a K_B, která se odvíjí od rozdělení χ. Zmíníme, že vhodnou volbou parametrů n, p a χ lze zajistit, aby pravděpodobnost toho, že strany obdrží různé klíče, byla dostatečně malá. Pro konkrétní volbu funkcí f, g a rec a pro příslušná tvrzení odkazujeme čtenáře například na [12], protože už se netýkají problému LWE a jejich technický charakter by mohl pouze znepřehlednit tuto část. V článku [10] je navíc předchozí metoda zobecněná, kdy z hodnot K_A, K_B extrahujeme více bitů. To je ale na úkor zvětšení pravděpodobnosti, že strany obdrží různé klíče. Další možností, jak zajistit, aby měl výsledný klíč více bitů, je použít místo vektorů $\mathbf{x}$, $\mathbf{y}$, $\mathbf{e}_A$, $\mathbf{e}_B$ matice. Potom budou K_A, K_B rovněž matice a z každého prvku těchto matic můžeme získat jeden bit (popřípadě více bitů) [10].

5.2 Bezpečnost

Útočníkem rozumíme pravděpodobnostní polynomiální algoritmus. Budeme se zabývat pouze pasivními útočníky, kteří pouze odposlouchávají komunikaci mezi stranami A, B a nijak do ní nezasahují. Po společném klíči K požadujeme, aby pro útočníka $\mathcal{A}$, který z komunikace mezi stranami A a B zná hodnoty $\mathbf{p}_A, \mathbf{p}_B$ a c, nebyl rozpoznatelný od klíče, který by byl zvolen náhodně. Bezpečnost schématu budeme vyjadřovat právě pomocí pravděpodobnosti, že se útočníkovi $\mathcal{A}$ podaří rozlišit, kdy je klíč K výsledkem výše popsané výměny a kdy je zvolen náhodně. Chtěli bychom, aby tato pravděpodobnost byla 1/2, tedy aby se mu klíč jevil jako náhodný. Budeme vycházet z článku [10]. Formálně použijeme následující experiment.

- Simulujeme část výměny:
  - Zvolíme $\mathbf{M} \leftarrow \mathcal{U}(\mathbb{Z}_p^{n \times n})$.
  - Zvolíme $\mathbf{x}, \mathbf{y}, \mathbf{e}_A, \mathbf{e}_B \leftarrow \chi^n$.
  - Zvolíme $e \leftarrow \chi$.
  - Spočítáme $\mathbf{p}_A = \mathbf{M}\mathbf{x} + \mathbf{e}_A \bmod p$.
  - Spočítáme $\mathbf{p}_B = \mathbf{M}^\top \mathbf{y} + \mathbf{e}_B \bmod p$.

  - Spočítáme $K_B = \mathbf{p}_A^\top \mathbf{y} + e \bmod p$.
  - Spočítáme $c = g(K_B)$.
- Položíme $K_0 = f(K_B)$ a $K_1 \leftarrow \mathcal{U}(\mathbb{Z}_2)$.
- Zvolíme $b \leftarrow \mathcal{U}(\mathbb{Z}_2)$.
- Útočník dostane pětici $(\mathbf{M}, \mathbf{p}_A, \mathbf{p}_B, c, K_b)$.

Úkolem útočníka $\mathcal{A}$ je zjistit, čemu se rovná b. Naznačíme, jak za předpokladu, že je HNF-decision-LWE$_{p,\chi}$ problém těžký, ukázat, že pravděpodobnost úspěchu útočníka $\mathcal{A}$ je blízko $1/2$. V kombinaci s redukcemi z předchozí části to bude znamenat, že schéma je bezpečné proti pasivním útočníkům za předpokladu, že zmíněné mřížové problémy jsou těžké.

K tomu uvažujme jiný experiment, kdy místo $\mathbf{p}_A = \mathbf{M}\mathbf{x} + \mathbf{e}_A \bmod p$ zvolíme $\mathbf{p}_A \leftarrow \mathcal{U}(\mathbb{Z}_p^n)$ a zbytek zůstane stejný. Kdyby se pravděpodobnost úspěchu útočníka $\mathcal{A}$ v takto pozměněném experimentu nezanedbatelně lišila od pravděpodobnosti úspěchu v původním experimentu, potom by útočník uměl s nezanedbatelnou výhodou rozlišit n dvojic z rozdělení $A_{\mathbf{x},\chi}$ a n dvojic z rozdělení $\mathcal{U}(\mathbb{Z}_p^n \times \mathbb{Z}_p)$, tedy by uměl řešit problém HNF-decision-LWE$_{p,\chi}$. Skutečně, dvojice $(\mathbf{M}^i, \mathbf{p}_A^i)$, kde $\mathbf{M}^i$ je i-tý řádek matice $\mathbf{M}$ a $\mathbf{p}_A^i$ je i-tá složka vektoru $\mathbf{p}_A$, odpovídá dvojici z rozdělení $A_{\mathbf{x},\chi}$ a $\mathbf{p}_A$ je jediné místo, kde se experimenty liší.

Nakonec uvažujme třetí experiment, který se od druhého liší tak, že místo $\mathbf{p}_B = \mathbf{M}^\top \mathbf{y} + \mathbf{e}_B \bmod p$ zvolíme $\mathbf{p}_B \leftarrow \mathcal{U}(\mathbb{Z}_p^n)$ a místo $K_B = \mathbf{p}_A^\top \mathbf{y} + e \bmod p$ zvolíme $K_B \leftarrow \mathcal{U}(\mathbb{Z}_p)$. Podobnou úvahou jako v předchozím odstavci dostaneme, že pravděpodobnost úspěchu útočníka $\mathcal{A}$ ve třetím experimentu je zanedbatelně blízko od pravděpodobnosti úspěchu ve druhém experimentu za předpokladu, že je problém HNF-decision-LWE$_{p,\chi}$ těžký. To byl také důvod, proč jsme při výpočtu K_B přičetli chybu e. Nyní se podíváme na pravděpodobnost úspěchu útočníka $\mathcal{A}$ ve třetím experimentu. Útočník obdrží $\mathbf{M}, \mathbf{p}_A, \mathbf{p}_B$, které byly zvoleny náhodně a nijak mu tedy nepomůžou. Kromě toho obdrží indicii c, která je nyní odvozena také z náhodné hodnoty, a tedy z vlastnosti 5.1 mu znalost c také nepomůže. Tedy pravděpodobnost, že útočník $\mathcal{A}$ uspěje ve třetím experimentu, je právě $1/2$. To znamená, že za předpokladu, že je problém HNF-decision-LWE$_{p,\chi}$ těžký, je pravděpodobnost, že útočník $\mathcal{A}$ uspěje v prvním experimentu, zanedbatelně blízko $1/2$. Tedy je schéma bezpečné proti pasivním útočníkům.

Závěr

V této práci jsme představili důležitý problém z mřížové kryptografie nazývaný LWE (*Learning with Errors*). Rozebrali jsme jeho varianty a ukázali jsme, že určité mřížové problémy se redukují na vhodné varianty problému LWE. To patří mezi hlavní důvody, proč je o problém LWE takový zájem. Věří se totiž, že příslušné mřížové problémy zůstanou těžké i pro kvantový počítač.

K tomuto účelu jsme nejprve ukázali, co jsou mříže, a představili jsme si jejich různé vlastnosti. Vyřešili jsme také několik cvičení týkajících se parametru mříže nazývaného pokrývající poloměr. V další části jsme zavedli pojem statistické vzdálenosti, která hraje v redukcích důležitou roli. Hodí se v situacích, kdy potřebujeme nahradit rozdělení pravděpodobnosti jeho aproximací. Příslušná tvrzení jsme se pokusili na rozdíl od [3] zobecnit, protože v redukcích nepracujeme pouze s diskrétními rozděleními pravděpodobnosti. Přidali jsme také jedno vlastní tvrzení, které jsme pro redukci potřebovali a nikde nenašli.

Nevýhodou schémat založených na problému LWE může být jejich neefektivita. V roce 2010 byla v článku [13] představena varianta ring-LWE, která tuto potíž z části řeší. Větší efektivita u schémat založených na této variantě je ale za cenu potenciálního snížení bezpečnosti, protože redukce jsou známy pouze pro problémy na speciálních typech mříží nazývaných ideálové mříže.

Redukce, které jsme představili, jsou založeny na variantě search-LWE, kdežto pro konkrétní schémata se hodí verze decision-LWE. V roce 2017 byla v článku [14] popsána redukce, která redukuje mřížové problémy na variantu decision-LWE přímo.

Jak varianta ring-LWE, tak nová redukce na problém decision-LWE jsou možnými pokračováními práce.

Seznam použité literatury

[1] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, September 2009.

[2] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: Extended abstract. In *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing*, STOC '09, pages 333–342, New York, NY, USA, 2009. ACM.

[3] Daniele Micciancio and S. Goldwasser. *Complexity of Lattice Problems*. Kluwer Academic Publishers, Norwell, MA, USA, 2002.

[4] Daniele Micciancio. *Point Lattices*. Poznámky k předmětu CSE206A: Lattices Algorithms and Applications, 2017. `http://cseweb.ucsd.edu/classes/fa17/cse206A-a/lec1.pdf`.

[5] Daniele Micciancio. *Minkowski's theorem*. Poznámky k předmětu CSE206A: Lattices Algorithms and Applications, 2017. `http://cseweb.ucsd.edu/classes/fa17/cse206A-a/lec2.pdf`.

[6] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM J. Comput.*, 37(1):267–302, apr 2007.

[7] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '09, pages 595–618, Berlin, Heidelberg, 2009. Springer-Verlag.

[8] Jan Rataj. Poznámky k předmětu NMMA203: Teorie míry a integrálu, 2018. `http://www.karlin.mff.cuni.cz/~rataj/TMI/TMI-text_2017.pdf`.

[9] Stanislaw Jarecki. *Handout 1*. Poznámky k předmětu ICS 280: Introduction to the Theory of Cryptography, 2004. `https://www.ics.uci.edu/~stasio/winter04/hnd1.pdf`.

[10] Joppe Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from lwe. Cryptology ePrint Archive, Report 2016/659, 2016. `https://eprint.iacr.org/2016/659`.

[11] Xiaodong Lin Jintai Ding, Xiang Xie. A simple provably secure key exchange scheme based on the learning with errors problem. Cryptology ePrint Archive, Report 2012/688, 2012. `https://eprint.iacr.org/2012/688`.

[12] Chris Peikert. Lattice cryptography for the internet. Cryptology ePrint Archive, Report 2014/070, 2014. `https://eprint.iacr.org/2014/070`.

[13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. Cryptology ePrint Archive, Report 2012/230, 2012. https://eprint.iacr.org/2012/230.

[14] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-lwe for any ring and modulus. Cryptology ePrint Archive, Report 2017/258, 2017. https://eprint.iacr.org/2017/258.