UNIVERZITET U NOVOM SADU
FAKULTET TEHNIČKIH NAUKA

Vajagić Jovana

KRIPTOGRAFIJA ZASNOVANA NA REŠETKAMA

- MASTER RAD -

Mentor
Prof. dr Vojin Šenk

Novi Sad, 2016.

Sadržaj

1 Uvod

Današnje vreme donelo je brz razvoj informacionih tehnologija i telekomunikacionih sistema, kao i hardvera i softvera, a samim tim i do povećanih mogućnosti zloupotrebe podataka koji se tim putevima prenose. Proizvođači često nemaju vremena za detaljno testiranje svoje opreme, pa se kao posledica javljaju propusti koji čine osnovu za rad potencijalnih napadača. Oni pak razvijaju sopstvene tehnike kako bi došli do značajnih podataka putem nesigurnih komunikacijskih kanala. Zato je uspostavljanje sigurnosti informacionih sistema u vidu zaštite podataka od neovlašćenog pristupa, podmetanja pogrešnih informacija, njihovog uništavanja i raznih zloupotreba izuzetno važna. Veliki broj preduzeća, državnih administracija, a posebno banaka pridaju veliku pažnju merama sigurnosti svojih podataka, a time i razvoju zaštitnih komunikacijskih mehanizama, najvažnijeg oblika ostvarenja sigurnosti. Tu na scenu stupa kriptografija, oblast koja se bavi proučavanjem raznih metoda za transformaciju proizvoljne poruke u oblik koji je čitljiv samo onom kome je ta poruka namenjena. Može se reći i da je kriptografija umeće sakrivanja informacija. Kiptografski protokoli čine osnovu svih protokola za zaštitu informacija koji se implementiraju na višim nivoima. Postoje simetrični i asimetrični kriptosistemi, a njihova razlika je u tome što simetrični algoritmi koriste jedan ključ za šifrovanje i dešifrovanje poruke, dok asimetrični koriste različite ključeve. U ovom radu biće opisani asimetrični kriptosistemi zasnovani na rešetkama.

Rešetke, kao algebarsku strukturu prvi su izučavali Žozef Luj Langranž (Joseph-Louis Lagrange) i Karl Fridrih Gaus (Carl Friedrich Gauss). Danas, mnogi poznati rezultati proučavanja ovih struktura, deo su oblasti *geometrija brojeva*. Primena rešetaka u kriptografiji proučava se tek 20-ak godina. Motivacija za proučavanje je između ostalog i potreba za različitošću matematičkih problema na kojima se temelje kriptosistemi i njihova sigurnost. Kriptografija zasnovana na rešetkama deo je oblasti kriptografije s javnim ključem. Velika prednost kriptosistema zasnovanih na rešetkama u odnosu na ostale kriptosisteme s javnim ključem je ta što su ovi kriptosistemi otporni na napade kvantnih algoritama. Dakle, ako želimo bezbednost informacija jednog dana kada ideja kvantnih kompjutera bude realizovana, treba na vreme detaljno da proučimo ovu oblast. Rešetke su tek nedavno korišćene u kompjuterskim algoritmima i kriptoanalizi, kao na primer 2009. godine, kada je Kreg Džentri (Craig Gentry) iz IBM-a predložio prvu potpuno homomorfnu enkripcijsku šemu baziranu na rešetkama. Pojam homomorfne enkripcije prvi put je predstavljen u [1] i omogućava nam da vršimo operacije nad šifratima bez poznavanja otvorenog teksta. Enkripcijske šeme koje su homomorfne u odnosu na samo jednu od operacija sabiranja i množenja zovu se parcijalne homomorfne enkripcijske šeme, dok je potpuno homomorfna enkripcijska šema homomorfna u odnosu na obe operacije. Tokom godina, razne enkripcijske šeme bile su predlagane i imale su ili operaciju sabiranja ili operaciju množenja šifrovanog teksta, ali ne obe. Džentrijeva šema je omogućila obe operacije. Međutim, iako predstavlja pravi teoretski iskorak, ova šema nije praktična.

U terminima sigurnosti, konstrukcije zasnovane na rešetkama mogu se podeliti na dva tipa. Prvi tip su praktični kriptosistemi, koji su vrlo efikasni, ali im nedostaje dokaz o sigurnosti. Drugi tip su sistemi koji imaju dokaz o svojoj sigurnosti, baziran na teško rešivom problemu u rešetki, ali s druge strane nisu dovoljno efikasni da bi se koristili u praksi. Koji su to teško rešivi problemi u rešetkama biće opisano u poglavlju 2.2. Dakle, razbijanje kriptosistema koji se zasniva na jednom takvom problemu impliciralo bi efikasan algoritam za rešavanje bilo koje instance tog problema. Međutim, najpoznatiji algoritmi koji rešavaju probleme u rešetkama su ili eksponencijalne složenosti ili daju lošu aproksimaciju rešenja. Takođe, ne postoji ni kvantni algoritam koji je znatno efikasniji u rešavanju ovih problema od algoritama koji nisu kvantni. Od Šorovog [1] otkrića kvantnog algoritma za

[1] Piter Šor (Peter Shor) rođen 1959. godine je američki matematičar, poznat po svom radu na teoriji kvantnih računara.

razlaganje celih brojeva na proste činioce 1994. godine bilo je mnogih pokušaja, ali bez uspeha.

U drugoj glavi biće rečeno nešto više o rešetkama kao algebarskim strukturama, njihovim osobinama i svojstvima. Takođe će biti spomenute bitnije teoreme koje važe, a neke od njih će biti i dokazane. Zatim ćemo se upoznati s teškim problemima u rešetkama na kojima se temelje kriptografske konstrukcije i videćemo kako se od dva najpoznatija problema, jedan redukuje na drugi. Takođe će biti opisana dva najpoznatija algoritma redukcije rešetke, tačnije baze rešetke, koja nam pružaju dobru bazu s kojom možemo bolje aproksimirati rešenja ovih problema.

U trećoj glavi biće predstavljena tri najpoznatija kriptosistema zasnovana na rešetkama, a to su Ajtai-Dvork (Ajtai-Dwork), Goldrajh-Goldvaser-Halevi (Goldreich-Goldwasser-Halevi) ili skraćeno GGH i NTRU kriptosistem. Svi oni se zasnivaju na teško rešivim problemima u rešetkama, iako je jedino GGH bio predstavljen preko rešetaka u originalnom radu. Videćemo da je matematika koja je u pozadini kriptosistema baziranih na rešetkama u suštini linearna algebra. U ovoj glavi će takođe biti predstavljen i praktičan deo master rada.

Četvrto poglavlje je pregled savremenijih rezultata iz oblasti kriptografije zasnovane na rešetkama. Dodatni problemi u rešetkama biće predstavljeni, kao i još jedan, noviji i možda najefikasniji kriptosistem. Takođe će biti definisane još neke klase rešetaka koje su poslednjih godina predmet izučavanja.

Na kraju će biti spomenuto gde se sve primenjuje ova oblast i šta nam to novo donosi što do sad nismo imali.

* * *

Posebno se zahvaljujem profesoru Vojinu Šenku koji mi je izašao u susret i prihvatio da bude moj mentor, kao i članovima komisije prof. dr Silviji Gilezan i prof. dr Kseniji Doroslovački na korisnim sugestijama. Izuzetnu zahvalnost dugujem profesoru Miodragu Miliću, bez čije pomoći ne bih imala priliku da odslušam predmet Kriptozaštita informacija, a samim tim ni da napišem ovaj rad. Takođe mu se zahvaljujem na velikoj pomoći u toku izrade rada, u vidu objašnjenja nejasnih pojmova i konstruktivnih saveta.

Najveću zahvalnost ipak dugujem svojim roditeljima, na podršci, strpljenju i potpunom verovanju u mene tokom studija. Takođe se zahvaljujem i svojim prijateljima, koji su uvek bili tu za mene.

2 Rešetke

2.1 Osnovne definicije i svojstva

Definicija 2.1.1 (Rešetka)**.** *Neka su $v_1, v_2, ..., v_m$ linearno nezavisni vektori prostora $\mathbb{R}^n$. Rešetka L generisana ovim vektorima sastoji se od svih linearnih kombinacija vektora $v_1, v_2, ..., v_m$ s celobrojnim koeficijentima, tj.*

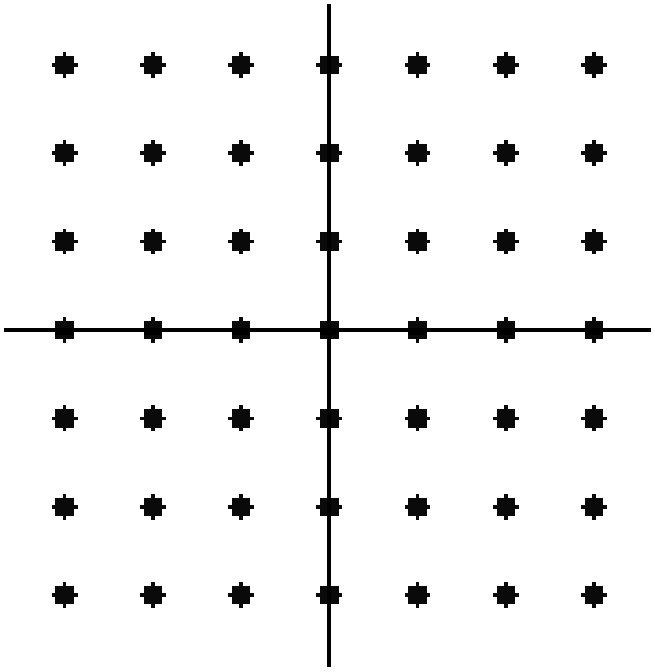
$$L = \{z_1v_1 + z_2v_2 + ... + z_mv_m | z_i \in \mathbb{Z}\}. \tag{2.1}$$

Skup vektora $\{v_1, v_2, ..., v_m\}$ zove se baza rešetke. Dimenzija rešetke je n, a rang rešetke je m. Ako je $m = n$, onda je rešetka kompletna ili punog ranga.

U terminima matrica rešetka se može zapisati na sledeći način

$$L = \{L(B)z | z \in \mathbb{Z}^m\}, \tag{2.2}$$

gde je sa $L(B)$ označena matrica čije su kolone koordinate vektora baze, a z je vektor kolone. Matricu $L(B)$ zovemo *generatorskom* matricom rešetke. Ako su vektori $v_1, v_2, ..., v_m$ iz skupa $\mathbb{Z}^n$, onda je L podskup od $\mathbb{Z}^n$ i zove se celobrojna (integralna) rešetka. Bilo koji podskup od L koji je i sam rešetka je podrešetka rešetke L. .



Slika 1: Rešetka $\mathbb{Z}^2$ koja sadrži sve vektore iz $\mathbb{R}^2$ s celobrojnim koordinatama.

Svaki skup linearno nezavisnih vektora koji generiše rešetku jeste njena baza. Primetimo da se vektorski prostor generisan sa $L(B)$, tj. sa $v_1, v_2, ..., v_m \in \mathbb{R}^n$ definiše slično kao rešetka.

$$\mathcal{L}(\{v_1, v_2, ..., v_m\}) = \{x_1v_1 + x_2v_2 + ... + x_mv_m | x_i \in \mathbb{R}\} = \{L(B)x | x \in \mathbb{R}^m\}, \tag{2.3}$$

gde je sa $\mathcal{L}$ označen lineal (ili linearni omotač) baznih vektora $v_1, v_2, ..., v_m$. Međutim, za razliku od vektorskih prostora, nije svaki maksimalni skup linearno nezavisnih vektora baza za rešetku. Naknadno će biti dat potreban i dovoljan uslov da bi neki skup bio baza.
Bilo koje dve baze imaju isti broj elemenata. Štaviše, svake dve baze su u relaciji na sledeći način [2].

Neka je $v_1, v_2, ..., v_m$ jedna baza i neka je $u_1, u_2, ..., u_m$ druga baza rešetke $L \subset \mathbb{R}^n$. Možemo zapisati vektore u_i kao linearne kombinacije baznih vektora v_i, $i = 1, ..., m$.

$$u_1 = z_{11}v_1 + z_{21}v_2 + ... + z_{m1}v_m,$$

$$u_2 = z_{12}v_1 + z_{22}v_2 + ... + z_{m2}v_m,$$

$$\vdots$$

$$u_m = z_{1m}v_1 + z_{2m}v_2 + ... + z_{mm}v_m.$$

U matričnom zapisu ovo je u stvari

$$[u_1 \ u_2 \ \cdots \ u_m] = [v_1 \ v_2 \ \cdots \ v_m] \begin{bmatrix} z_{11} & z_{12} & \cdots & z_{1m} \\ z_{21} & z_{22} & \cdots & z_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ z_{m1} & z_{m2} & \cdots & z_{mm} \end{bmatrix}.$$

Ako bismo pak želeli da izrazimo vektore $v_1, v_2, ..., v_m$ preko baznih vektora $u_1, u_2, ..., u_m$, morali bismo da invertujemo matricu

$$U = \begin{bmatrix} z_{11} & z_{12} & \cdots & z_{1m} \\ z_{21} & z_{22} & \cdots & z_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ z_{m1} & z_{m2} & \cdots & z_{mm} \end{bmatrix}.$$

Takođe, s obzirom na to da su koeficijenti u tim relacijama celobrojni, elementi matrice U^{-1} moraju biti celi brojevi. Stoga je

$$det(U)det(U^{-1}) = det(UU^{-1}) = det(E) = 1,$$

gde su $det(U)$ i $det(U^{-1})$ celi brojevi, te je jedino moguće da je $det(U^{-1}) = \pm 1$. Dakle svake dve baze za rešetku L su u relaciji preko matrice s celobrojnim elementima i determinantom ± 1. Tačnije, za svake dve baze koje generišu rešetku i njihove odgovarajuće matrice $L(B_1)$ i $L(B_2)$ važi relacija

$$L(B_1) = L(B_2)U, \tag{2.4}$$

gde je U unimodularna matrica, odnosno celobrojna matrica s determinantom ± 1. Kažemo i da su tada baze ekvivalentne.

Primer 2.1.1. Posmatrajmo trodimenzionalnu rešetku $L \subset \mathbb{R}^3$ generisanu sa sledeća tri vektora:

$$v_1 = (7, 5, -2), \ \ v_2 = (5, 7, 0), \ \ v_3 = (2, -3, 7).$$

Formiramo matricu $L(B_1)$.

$$L(B_1) = \begin{bmatrix} 7 & 5 & 2 \\ 5 & 7 & -3 \\ -2 & 0 & 7 \end{bmatrix}.$$

Sada uvodimo tri nova vektora u L preko formula:

$$u_1 = v_1 + v_3, \ \ u_2 = v_1 + v_2, \ \ u_3 = v_1 + v_2 + v_3.$$

Ovo je ekvivalentno množenju matrice $L(B_1)$ s desne strane matricom

$$U = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Vektore u_1, u_2 i u_3 nalazimo kao kolone matrice

$$L(B_2) = L(B_1)U = \begin{bmatrix} 9 & 12 & 14 \\ 2 & 12 & 9 \\ 5 & -2 & 5 \end{bmatrix}.$$

Matrica U ima determinantu 1, što znači da su vektori u_1, u_2 i u_3 takođe baza za L. Inverzna matrica za U je

$$U^{-1} = \begin{bmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ -1 & 1 & 1 \end{bmatrix}.$$

Njena determinanta je takođe 1. Kolone ove matrice nam govore kako da izrazimo stare vektore preko novih, tj.

$$v_1 = u_1 + u_2 - u_3, \;\; v_2 = u_3 - u_1, \;\; v_3 = u_3 - u_2.$$

Lema 2.1.1. *Dve baze su ekvivalentne ako i samo ako se vektori jedne mogu izraziti preko vektora druge baze, na sledeće načine:*

- $v_i \leftrightarrow v_j$ *(permutacijom starih vektora)*
- $v_i \to -v_i$ *(negacijom)*
- $v_i \to v_i + kv_j$, *gde je* $i \neq j$ *i* $k \in \mathbb{Z}$.

Definicija 2.1.2. *Neka je* $(L, +)$ *podgrupa od grupe* $(\mathbb{R}^n, +)$. *Podgrupa* $(L, +)$ *je diskretna ako postoji pozitivan broj* a *tako da važi sledeće svojstvo: za svako* $v \in L$,

$$L \cap \{w \in \mathbb{R}^n : ||v - w|| < a\} = \{v\}, \tag{2.5}$$

gde je sa $\|\cdot\|$ *označena euklidska norma.*

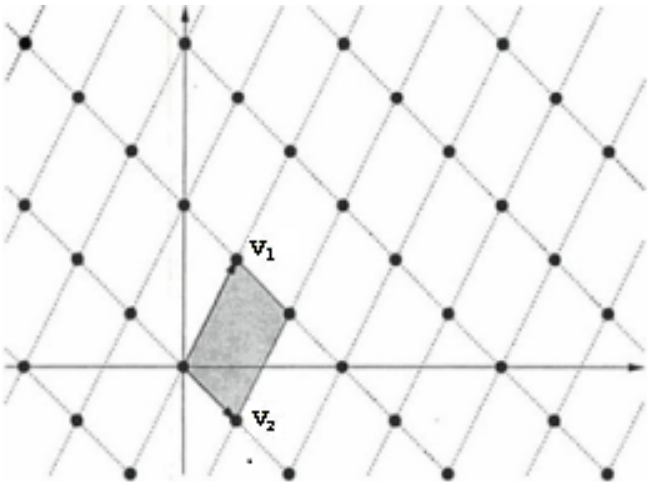
Dakle, oko svake tačke rešetke može se opisati otvorena lopta poluprečnika a tako da unutar te lopte nema drugih tačaka rešetke. Ovo nas dovodi do druge definicije.

Definicija 2.1.3 (Rešetka)**.** *Diskretna aditivna pogrupa grupe* $\mathbb{R}^n$ *naziva se rešetka.*

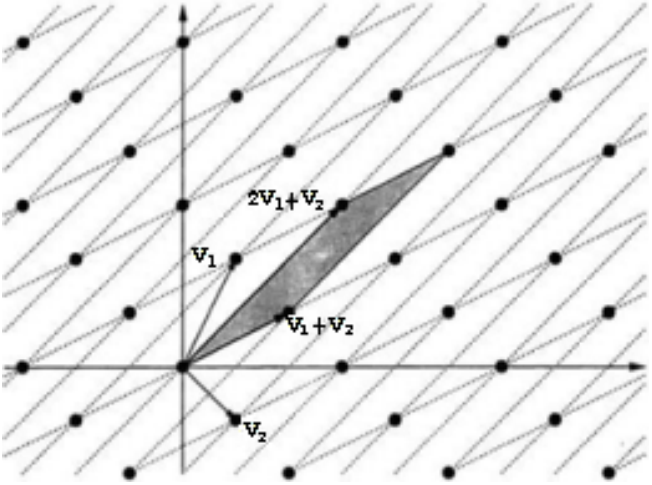
Napomena 1. *Definicija 2.1.1 i 2.1.3 su ekvivalentne.*

Lema 2.1.2. *Neka je* $L \subset \mathbb{R}^n$ *rešetka. Tada važe sledeća svojstva:*

1. L *je zatvoren skup, dakle* L *nema tačaka nagomilavanja van* L, *stoga ih nema uopšte.*
2. *Ako je* $S \subseteq \mathbb{R}^n$ *neki ograničen skup, onda je* $L \cap S$ *končan.*
3. L *je prebrojiv.*



Slika 2: Celobrojna rešetka s dva bazna vektora koji je generišu, $v_1 = (1, 2)$ i $v_2 = (1, -1)$.



Slika 3: Celobrojna rešetka sada s druga dva bazna vektora, izražena preko prethodnih, $v_1' = v_1 + v_2 = (2, 1)$ i $v_2' = 2v_1 + v_2 = (3, 3)$.

Ako je $L \subset \mathbb{R}^n$ rešetka ranga n s bazom $v_1, v_2, ..., v_n$, onda je fundamentalni domen (paralelopiped) za L koji odgovara ovoj bazi dat sa

$$\mathcal{F}(v_1, ..., v_n) = \{t_1 v_1 + ... + t_n v_n | 0 \leq t_i < 1, i = 1, ..., n\}. \tag{2.6}$$

Translacije osnovnog domena pokrivaju celo $\mathbb{R}^n$, odnosno važi naredna teorema.

Teorema 2.1.1. *Neka je L kompletna rešetka u $\mathbb{R}^n$ i $\mathcal{F}$ njen osnovni domen. Tada za svaki vektor $w \in \mathbb{R}^n$ postoje jedinstveni vektori $u \in \mathcal{F}$ i $v \in L$ takvi da je $w = u + v$. Stoga, sve translacije osnovnog domena*

$$\mathcal{F} + v = \{u + v | u \in \mathcal{F}\}$$

pokrivaju ceo $\mathbb{R}^n$.

Dokaz. Neka je $v_1, v_2, ..., v_n$ baza rešetke L i $\mathcal{F}(v_1, v_2, ..., v_n)$ njen osnovni domen. S obzirom na to da su $v_1, v_2, ..., v_n$ linearno nezavisni u $\mathbb{R}^n$, oni čine bazu za $\mathbb{R}^n$. Odatle sledi da se svaki vektor w može zapisati kao linearna kombinacija ovih vektora, odnosno, $w = a_1 v_1 + a_2 v_2 + ... + a_n v_n$, gde

$a_i \in \mathbb{R}$, $i = 1, 2, ..., n$. Dalje, svako a_i može se zapisati u narednom obliku $a_i = t_i + z_i$, za $0 \leq t_i < 1$ i $z_i \in \mathbb{Z}$. Sada je

$$w = \underbrace{t_1 v_1 + t_2 v_2 + ... + t_n v_n}_{\in \mathcal{F}} \; + \; \underbrace{z_1 v_1 + z_2 v_2 + ... + z_n v_n}_{\in L}.$$

Dakle, vektor w može se zapisati u željenoj formi. Još treba pokazati jedinstvenost zapisa.
Pretpostavimo da se w može zapisati i kao $w = u' + v'$. Neka je $u' = t_1' v_1 + ... + t_n' v_n$, a $v' = z_1' v_1 + ... + z_n' v_n$. Tada je

$$(t_1 + z_1)v_1 + (t_2 + z_2)v_2 + ... + (t_n + z_n)v_n =$$

$$(t_1' + z_1')v_1 + (t_2' + z_2')v_2 + ... + (t_n' + z_n')v_n.$$

Kako su vektori $v_1, v_2, ..., v_n$ linearno nezavisni sledi da mora važiti jednakost $t_i + z_i = t_i' + z_i'$, za sve $i = 1, 2, ..., n$. Dakle, broj

$$t_i - t_i' = z_i' - z_i$$

je ceo. Znamo da važi $0 \leq t_i < 1$, pa je $t_i - t_i'$ ceo broj jedino ako je $t_i = t_i'$. Stoga je i $u = u'$. Odavde sledi da je $v = w - u = w - u' = v'$ čime je dokaz kompletiran. □

Sada kada je definisan osnovni domen, vratimo se na trenutak na bazu rešetke L. Potreban i dovoljan uslov da skup nezavisnih vektora rešetke formira bazu dat je narednom teoremom.

Teorema 2.1.2. *Neka je $L \subset \mathbb{R}^n$ rešetka ranga m i neka su $v_1, v_2, ..., v_m$ vektori rešetke L koji su linearno nezavisni. Tada oni čine bazu rešetke L ako i samo ako ne postoji ne-nula vektor rešetke w takav da $w \in \mathcal{F}(v_1, v_2, ..., v_m)$.*

Dokaz. ($\Longrightarrow$) Neka je $i-$ti vektor baze $v_i = (v_{1i}, v_{2i}, ..., v_{ni})$, a matrica $B = \{v_{ij}\}_{n \times m}$, odnosno matrica čije su kolone koordinate ovih vektora. Pošto je B po pretpostavci generatorska matrica rešetke L, svaki vektor rešetke može se zapisati kao linearna kombinacija baznih vektora s celobrojnim koeficijentima

$$w = \sum_{i=1}^{m} z_i v_i, \quad z_i \in \mathbb{Z}$$

ili u terminima matrica $w = Bz$, gde je z vektor kolone. Ako $w \in \mathcal{F}(v_1, v_2, ..., v_m) = \mathcal{F}(B)$, onda je $0 \leq z_i < 1$ po definiciji i stoga je jedino moguće da je $z_i = 0$ za sve $1 \leq i \leq m$. Dakle, jedini vektor rešetke koji pripada fundamentalnom domenu je nula vektor.
($\Longleftarrow$) Drugi smer dokazuje se kontrapozicijom. Pretpostavimo da B nije generatorska matrica rešetke L. To znači da mora postojati vektor $u \in L$ takav da u nije linearna kombinacija vektora v_i, $i = 1, ..., m$ s celobrojnim koeficijentima. Pošto su $v_1, v_2, ..., v_m$ linearno nezavisni vektori, oni čine bazu u $\mathbb{R}^m$, te se vektor u može zapisati kao

$$u = \sum_{i=1}^{m} r_i v_i, \quad r_i \in \mathbb{R},$$

gde bar jedno r_i nije ceo broj. Uzmimo u obzir sledeći vektor

$$u' = \sum_{i=1}^{m} \lfloor r_i \rfloor v_i, \quad r_i \in \mathbb{R}.$$

Koeficijenti $\lfloor r_i \rfloor$ su celi brojevi, stoga ovaj vektor pripada L. Kako je L aditivna podgrupa, razlika ova dva vektora takođe pripada L, odnosno vektor

$$w = u - u' = \sum_{i=1}^{m} (r_i - \lfloor r_i \rfloor) v_i \quad \in L.$$

Kako je $0 \leq r_i - \lfloor r_i \rfloor < 1$, vektor w pripada fundamentalnom domenu $\mathcal{F}$. Takođe, ovaj vektor je različit od nula vektora, s obzirom na to da bar jedno r_i nije ceo broj, te je $r_i - \lfloor r_i \rfloor > 0$ za neko i. Dakle, $w \in L$ je ne-nula vektor koji pripada $\mathcal{F}(B)$, što je i trebalo dokazati.

□

Definicija 2.1.4 (Determinanta rešetke)**.** *Neka je L kompletna rešetka u $\mathbb{R}^n$ s bazom $v_1, v_2, ..., v_n$ i neka je $\mathcal{F}$ njen osnovni paralelopiped u odnosu na tu bazu. Tada se n-dimenzionalna zapremina od $\mathcal{F}$ naziva determinanta od L i označavamo je sa $det(L)$.*

Ako se posmatra paralelopiped $\mathcal{F}$ čije su ivice vektori baze rešetke, može se videti da se najveća zapremina postiže ako su ti vektori po parovima ortogonalni. Specijalno, važi naredna lema.

Lema 2.1.3 (Adamarova nejednakost)**.** *Neka je L rešetka u $\mathbb{R}^n$. Za proizvoljnu bazu $v_1, v_2, ..., v_n$ i fundamentalni paralelopiped $\mathcal{F}$ u odnosu na tu bazu važi*

$$det(L) = Vol(\mathcal{F}) \leq \|v_1\| \|v_2\| \cdots \|v_n\|, \tag{2.7}$$

gde je sa $Vol(\mathcal{F})$ označena zapremina osnovnog paralelopipeda.

Što su vektori više ortogonalni međusobno, to je Adamarova nejednakost bliža jednakosti.

Teorema 2.1.3. *Neka je $L \subset \mathbb{R}^n$ kompletna rešetka i neka je $v_1, v_2, ..., v_n$ baza za L, a $L(B)$ odgovarajuća generatorska matrica. Dalje, neka je $\mathcal{F} = \mathcal{F}(v_1, v_2, ..., v_n)$ njen osnovni paralelopiped u odnosu na tu bazu. Njegova zapremina data je formulom*

$$Vol(\mathcal{F}) = det(L) = |detL(B)|. \tag{2.8}$$

Dokaz. Zapremina paralelopipeda može se izračunati na sledeći način

$$Vol(\mathcal{F}) = \int_{\mathcal{F}} dx_1 dx_2 ... dx_n,$$

odnosno kao integral konstantne funkcije 1 nad oblasti $\mathcal{F}$. Podsetimo se, osnovni domen je definisan sa $\mathcal{F}(v_1, ..., v_n) = \{t_1 v_1 + ... + t_n v_n | 0 \leq t_i < 1, i = 1, ..., n\}$. Dakle želimo da izrazimo $x = (x_1, ..., x_n)$ preko $t = (t_1, ..., t_n)$, te je $(x_1, ..., x_n) = t_1 v_1 + ... + t_n v_n$. U terminima matrica, smena je data sa $x = L(B)t$, gde su x i t vektori kolona. Jakobijeva matrica ove smene promenljivih je upravo $L(B)$. Fundamentalni domen dobija se preko kocke $K_n = [0, 1]^n$ i Jakobijeve matrice, odakle sledi

$$\int_{\mathcal{F}} dx_1 dx_2 ... dx_n = \int_{L(B)K_n} dx_1 dx_2 ... dx_n = \int_{K_n} |det\big(L(B)\big)| dt_1 dt_2 ... dt_n$$

$$= |det\big(L(B)\big)| \underbrace{Vol(K_n)}_{1} = |det\big(L(B)\big)|.$$

□

Posledica 2.1.1. *Neka je $L \subset \mathbb{R}^n$ kompletna rešetka. Tada svi njeni fundamentalni domeni imaju istu zapreminu. Stoga, determinanta rešetke L ne zavisi od domena koji je korišćen za njeno izračunavanje.*

Dokaz. Neka su $L(B_1)$ i $L(B_2)$ matrice koje odgovaraju bazama $v_1, v_2, ..., v_n$ i $u_1, u_2, ..., u_n$ rešetke L, respektivno. Iz relacije date jednačinom 2.4 sledi da je

$$\begin{aligned} & Vol\big(\mathcal{F}(v_1, v_2, ..., v_n)\big) \\ &= |det\big(L(B_1)\big)| \\ &= |det\big(L(B_2)U\big)| \\ &= |det\big(L(B_2)\big)||det(U)| \\ &= |det\big(L(B_2)\big)| \\ &= Vol\big(\mathcal{F}(u_1, u_2, ..., u_n)\big) \end{aligned}$$

□

Napomena 2. *Još jedan način računanja determinante rešetke je preko formule*

$$det(L) = \sqrt{det\big(L(B)^T L(B)\big)}. \tag{2.9}$$

Definicija 2.1.5 (Dualna rešetka)**.** *Za datu rešetku $L \subset \mathbb{R}^n$ i njenu proizvoljnu bazu $v_1, v_2, ..., v_m$ dualna rešetka definiše se kao*

$$L^x = \{y \in \mathcal{L}(\{v_1, v_2, ..., v_m\}) | \langle x, y\rangle \in \mathbb{Z}, \textit{za sve } x \in L\}. \tag{2.10}$$

Definicija 2.1.6 (Ortogonalna rešetka)**.** *Za datu rešetku $L \subset \mathbb{R}^n$ ortogonalna rešetka se definiše na sledeći način*

$$L^{\perp} = \{y \in \mathbb{R}^n | \langle x, y\rangle = 0, \textit{za sve } x \in L\}. \tag{2.11}$$

Definicija 2.1.7 (Modularna (q-arna rešetka))**.** *Rešetka L koja zadovoljava*

$$q\mathbb{Z}^n \subseteq L \subseteq \mathbb{Z}^n, \tag{2.12}$$

gde je q ceo broj (po mogućnosti prost) naziva se modularna ili q-arna rešetka.

Kako je svaka rešetka zatvorena za sabiranje, vektor $z \in \mathbb{Z}^n$ pripada $q-$arnoj rešetki L ako i samo ako je $R_q[z]$ (ostatak pri deljenju z sa q) takođe u rešetki. Bilo koja celobrojna rešetka $L \subseteq \mathbb{Z}^n$ je q-arna rešetka za neko q koje je celobrojni umnožak determinante rešetke (videti [3]).
Neka je data matrica $A \in \mathbb{Z}_q^{n\times m}$, gde su q, m i n celi brojevi. Dve vrste $m-$dimenzionalnih $q-$arnih rešetaka date su narednom definicijom.

Definicija 2.1.8.

$$\Lambda_q(A) = \{y \in \mathbb{Z}^m |\ \ y = R_q[A^T s] \textit{ za neko } s \in \mathbb{Z}^n\}; \tag{2.13}$$

$$\Lambda_q^{\perp}(A) = \{y \in \mathbb{Z}^m |\ \ R_q[Ay] = 0\}. \tag{2.14}$$

Prva rešetka generisana je vektorima vrsta matrice A, dok druga sadrži sve vektore koji su ortogonalni u odnosu na vektore vrsta matrice A po modulu q.

Ove dve rešetke su međusobno dualne, odnosno važi

$$\Lambda_q^{\perp}(A) = q\cdot \Lambda_q(A)^x \quad \text{i} \tag{2.15}$$

$$\Lambda_q(A) = q\cdot \Lambda_q^{\perp}(A)^x. \tag{2.16}$$

2.2 Klasični problemi kod rešetaka

Postoji nekoliko teško rešivih problema u rešetkama, među kojima se najznačajnim smatraju dva problema i oni će, pored ostalih problema, biti predstavljeni u ovom odeljku. To su problem najbližeg vektora (CVP) i problem najkraćeg vektora (SVP). Za prvi problem se zna da je NP-težak, naime prvi dokaz pružio je Piter van Emde Boas (Peter van Emde Boas) 1981. godine, dok se za drugi zna da nije teži od prvog (u istoj dimenziji). Algoritmi za njihovo rešavanje nazivaju se algoritmi redukcije rešetke. Najbolji algoritmi za rešavanje ovih problema su ili eksponencijalne složenosti ili daju loše aproksimativne rezultate. U ovom poglavlju, pored spomenutih problema, biće predstavljene i neke njihove varijante kao i još nekoliko zanimljivih problema. Nadalje će se u obzir uzimati uglavnom celobrojne rešetke, odnosno rešetke čiji su bazni vektori s celobrojnim koordinatama.

Neka je $L \subseteq \mathbb{Z}^n$ netrivijalna rešetka, odnosno rešetka koja sadrži bar jedan ne-nula vektor x. Kako je skup $S = \overline{\mathcal{B}(0, \|x\|)}$ ograničen, sledi da je onda $L \cap S$ konačan. Pošto $x \in L \cap S$, to znači da skup $L \cap S$ sadrži bar jedan ne-nula vektor. Dakle, ovaj skup je neprazan i konačan, pa stoga postoji vektor $v \in L$ takav da je $\|v\| = \min\limits_{x \in L \setminus \{0\}} \|x\|$, gde je $\|\cdot\|$ euklidska norma.
Ovo nas dovodi do prvog problema.

Definicija 2.2.1 (Problem najkraćeg vektora (SVP))**.** *Ako je data baza rešetke $L \subseteq \mathbb{Z}^n$, naći ne-nula vektor $v \in L$ takav da važi*

$$\|v\| = \min_{x \in L \setminus \{0\}} \|x\|.$$

Definicijom problema se ne zahteva da najkraći vektor bude jedinstven. Dovoljno je naći jedan koji zadovoljava dati uslov. Dužina najkraćeg vektora obeležava se sa $\lambda_1(L)$.

Primer 2.2.1. U $\mathbb{Z}^2$ sva četiri vektora $(1, 0)$, $(0, 1)$, $(-1, 0)$ i $(0, -1)$ jesu rešenje SVP problema.

U praksi se često ne zahteva zaista najkraći vektor, već vektor koji je "dovoljno kratak". Šta to tačno znači govori nam naredna definicija.

Definicija 2.2.2 (Aproksimativni problem najkraćeg vektora (SVP$_\gamma$))**.** *Ako je data baza rešetke $L \subseteq \mathbb{Z}^n$ i aproksimativni faktor $\gamma \geq 1$, naći ne-nula vektor $v \in L$ takav da važi*

$$\|v\| \leq \gamma \min_{x \in L \setminus \{0\}} \|x\|.$$

Dakle, "dovoljno kratak" vektor je onaj koji nije više od γ puta duži od najkraćeg vektora u rešetki. Faktor γ može biti konstanta ili funkcija od dimenzije rešetke, tj. $\gamma = \gamma(n)$. Drugi teško rešiv problem je problem najbližeg vektora.

Definicija 2.2.3 (Problem najbližeg vektora (CVP))**.** *Ako je data baza rešetke $L \subseteq \mathbb{Z}^n$ i vektor $w \in \mathbb{R}^n$ koji ne pripada L, naći vektor $v \in L$ koji je najbliži vektoru w, odnosno vektor koji mimimizuje euklidsku normu $\|w - v\|$. Vektor w naziva se vektor meta (engl. target vector).*

Označimo sa $min_r(w, v)$ to minimalno rastojanje. Kao i kod prvog problema, nije uvek neophodno naći najbliži vektor, već vektor koji je "dovoljno blizu".

Definicija 2.2.4 (Aproksimativni problem najbližeg vektora (CVP$_\gamma$))**.** *Ako je data baza rešetke $L \subseteq \mathbb{Z}^n$, vektor $w \in \mathbb{R}^n$ koji ne pripada L i aproksimativni faktor γ, naći ne-nula vektor $u \in L$ takav da važi $\|w - u\| \leq \gamma \min_r(w, v)$.*

Poznato je da je CVP$_\gamma$ problem NP-težak za bilo koji konstantan faktor. Jedino u slučaju kada je aproksimativni faktor skoro eksponencijalan $(2^{O(n \log\log n / \log n)})$ SVP$_\gamma$ i CVP$_\gamma$ su rešivi u polinomijalnom vremenu (videti poglavlje 2.4).

Naredni problem uveo je Miklos Ajtai[2] (Miklós Ajtai) u svom radu [4].

Definicija 2.2.5 (Problem jedinstvenog najkraćeg vektora (uSVP$_\gamma$))**.** *Ako je data baza $L(B)$ kompletne rešetke $L \subseteq \mathbb{Z}^n$ i faktor raskoraka γ (engl. gap factor), naći najkraći ne-nula vektor $v \in L$ takav da važi da je bilo koji vektor $x \neq v$, $x \in L$ s osobinom $\|x\| \leq \gamma\|v\|$ paralelan sa v.*

Ajtai je pokazao da bi rešavanje SVP$_\gamma$ problema za slučajno odabrane rešetke iz određene klase impliciralo rešavanje problema jedinstvenog najkraćeg vektora za bilo koju instancu problema (videti poglavlje 3.1).

Definicija 2.2.6 (Odlučujući problem najkraćeg vektora (GapSVP$_\gamma$))**.** *Neka je data baza $L(B)$ rešetke $L \subseteq \mathbb{Z}^n$ ranga m, realni broj r i aproksimativni faktor γ. Ako je $\lambda_1(L) \leq r$ odgovor je DA, a ako je $\lambda_1(L) > \gamma r$ odgovor je NE.*

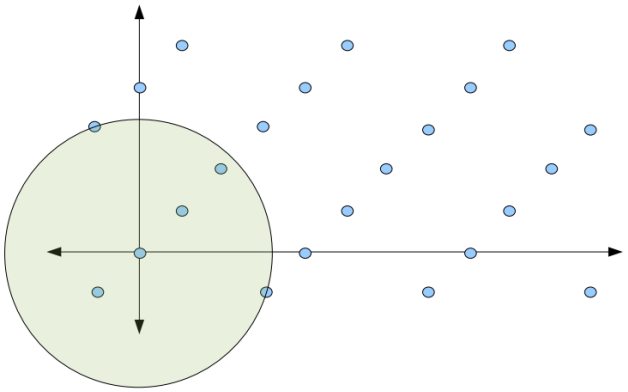
Još neki interesantni problemi u rešetkama biće spomenuti, ali pre toga treba definisati pojam sukcesivnog minimuma.

Definicija 2.2.7 (i-ti sukcesivni minimum)**.** *Neka je L n-dimenzionalna rešetka ranga m. Za $i = 1, 2, ..., m$ i-ti sukcesivni minimum je*

$$\lambda_i(L) = inf\{r|dim(\mathcal{L}(L \cap \overline{B(0,r)})) \geq i\}, \tag{2.17}$$

gde je $\overline{B(0,r)} = \{x \in \mathbb{R}^m | \|x\| \leq r\}$ zatvorena lopta s centrom u 0 poluprečnika r, a norma je euklidska, tj. ℓ_2.

Dakle, u pitanju je poluprečnik najmanje lopte s centrom u nuli, koja sadrži i linearno nezavisnih vektora rešetke. Nalaženje takvog r definiše upravo problem najkraćih nezavisnih vektora (slika 4) odnosno SIVP (engl. *Shortest Independent Vector Problem*).



Slika 4: SIVP problem.

U praksi se ipak više primenjuje aproksimativni problem.

Definicija 2.2.8 (Aproksimativni problem najkraćih nezavisnih vektora (SIVP$_\gamma$))**.** *Ako je data baza $L(B)$ rešetke $L \subseteq \mathbb{Z}^n$ ranga m i aproksimativni faktor γ, naći skup linearno nezavisnih vektora $u_1, u_2, ..., u_m$ koji zadovoljavaju*

$$\max_i \|u_i\| \leq \gamma\lambda_m(L), \quad i = 1, 2, ..., m,$$

gde je $\lambda_m(L)$ $m-$ti sukcesivni minimum.

[2]Miklos Ajtai, rođen 2.7.1946, je mađarski naučnik zaposlen u IBM Almaden istraživačkom centru. Glavna oblast istraživanja mu je teorija kompleksnosti.

Pokazano je da je ovaj problem NP-težak za faktor $\gamma = n^{1/\log\log n}$ [5]. Dužina najkraćeg vektora može se definisati i na sledeći način.

Definicija 2.2.9 (Prvi sukcesivni minimum)**.** *Minimalno rastojanje između bilo koje dve tačke rešetke naziva se prvi sukcesivni minimum i jednak je dužini najkraćeg vektora u rešetki, odnosno važi*

$$\lambda_1(L) = \min_{x \in L \setminus \{0\}} \|x\|. \tag{2.18}$$

Dakle, λ_1 je u stvari poluprečnik najmanje lopte s centrom u nuli, koja sadrži ne-nula vektor rešetke. Pitanje je da li je moguće odrediti ga. Slično, λ_2 je poluprečnik najmanje lopte s centrom u nuli, koja sadrži dva linearno nezavisna vektora itd.

Naredni problem uveo je Ajtai u svom radu [4], gde je kao i u slučaju problema jedinstvenog najkraćeg vektora pokazao da rešenje SVP problema u nasumičnoj rešetki povlači rešenje ovog problema.

Definicija 2.2.10 (Aproksimativni problem najkraćeg rastojanja)**.** *Ako je data baza $L(B)$ rešetke $L \subseteq \mathbb{Z}^n$ ranga m i aproksimativni faktor $\gamma > 0$, naći vrednost λ*

$$\lambda_1(L) \leq \lambda \leq \gamma\lambda_1(L),$$

takvu da postoji $v \in L$ sa osobinom $\|v\| = \lambda$.

Ako se uzme da je $\gamma = 1$ dobijamo tačnu verziju problema. Sledeći problem je u stvari jedna verzija CVP problema.

Definicija 2.2.11 (Dekodiranje ograničenog rastojanja (BDD))**.** *Ako je data baza $L(B)$ rešetke $L \subseteq \mathbb{Z}^n$, parametar rastojanja r i vektor meta $x \in \mathbb{R}^n$ takav da je $d(x, L) < r\lambda_1(L)$, naći vektor rešetke $u \in L$ takav da važi*

$$\|x - u\| = d(x, L).$$

Pokazano je da je ovaj problem NP-težak za parametar rastojanja $r > \frac{1}{\sqrt{2}}$ [6]. Što je parametar r veći, ovaj problem postaje teži.

Posebno je zanimljivo ispitivanje problema najkraće baze, jer nam takva baza daje bolje rezultate.

Definicija 2.2.12 (Problem najkraće baze (SBP))**.** *Naći bazu $v_1, v_2, ..., v_n$ za rešetku L, koja je najkraća u nekom smislu. Na primer, možemo zahtevati da baza minimizuje*

$$\max_{1 \leq i \leq n} \|v_i\| \quad \textit{ili} \quad \sum_{i=1}^{n} \|v_i\|^2.$$

Definicija 2.2.13 (Aproksimativni problem najkraće baze (SBP_γ))**.** *Ako je data rešetka $L \subseteq \mathbb{Z}^n$ ranga m i aproksimativni faktor $\gamma > 0$, naći bazu $v_1, v_2, ..., v_m$ takvu da*

$$\max_{1 \leq i \leq m} \|v_i\| \leq \gamma \max_{1 \leq i \leq m} \|v_i'\|,$$

važi za sve baze $v_1', v_2', ..., v_m'$ rešetke L.

Teorijski rezultati

Teorema 2.2.1 (O najbližem vektoru)**.** *Neka je V potprostor od $\mathbb{R}^n$ i neka je w vektor u $\mathbb{R}^n$. Ako je $v_1, v_2, ..., v_m$ ortonormirana baza za V, tada postoji jedinstven vektor $v \in V$ koji je najbliži vektoru w, dat sa:*

$$v = \sum_{i=1}^{m} \langle w, v_i \rangle v_i. \tag{2.19}$$

Za vektorski potprostor V i vektor $w \in \mathbb{R}^n$, ova teorema u stvari daje algoritam za nalaženje najbližeg vektora u prostoru V. Prvo se odredi ortonormirana baza za V, a zatim se iskoristi data formula. Ako je L rešetka u $\mathbb{R}^n$, možda ne postoji ortogonalna (ortonormirana) baza za nju. Stoga, ako bismo hteli da nađemo najbliži vektor $v \in L$ nekom datom vektoru $w \in \mathbb{R}^n$, ne bismo imali konkretan algoritam da to učinimo.

Teorema 2.2.2 (Bličfildova teorema)**.** *Za bilo koju kompletnu rešetku $L \subset \mathbb{R}^n$ i skup $S \subset \mathbb{R}^n$ čija je zapremina $Vol(S) > det(L)$ postoje dve različite tačke $z_1, z_2 \in S$ tako da $z_1 - z_2 \in L$.*

Teorema 2.2.3 (Teorema Minkovskog)**.** *Neka je L kompletna rešetka u $\mathbb{R}^n$ (ne neophodno celobrojna). Neka je $S \subset \mathbb{R}^n$ simetričan u odnosu na koordinatni početak, konveksan podskup čija zapremina zadovoljava*

$$Vol(S) > 2^n det(L).$$

Tada S sadrži ne-nula vektor rešetke L. Takođe, ako je S zatvoren podskup od $\mathbb{R}^n$, onda rezultat važi i za $Vol(S) \geq 2^n det(L)$.

Kao posledicu imamo Hermitovu teoremu koja nam obezbeđuje gornju granicu za najkraći vektor, čiji se dokaz zasniva na teoremi Minkovskog.

Teorema 2.2.4 (Hermitova teorema)**.** *Neka je L kompletna celobrojna rešetka. Tada postoji vektor $v \in L$ koji zadovoljava sledeću nejednakost*

$$\|v\| \leq \sqrt{n} \sqrt[n]{det(L)}.$$

Dokaz. Neka je $L \subset \mathbb{R}^n$ rešetka i neka je K kocka u $\mathbb{R}^n$ centralizovana u nuli, čija je ivica $2\sqrt[n]{det(L)}$, odnosno

$$K = \{(x_1, x_2, ..., x_n) \in \mathbb{R}^n : \ -\sqrt[n]{det(L)} \leq x_i \leq \sqrt[n]{det(L)}, \text{ za sve } i = 1, 2, ..., n\}.$$

Ova kocka je centralno-simetričan, konveksan i zatvoren skup sa zapreminom $Vol(K) = 2^n det(L)$. Dakle, ona zadovoljava uslove teoreme Minkovskog, a odatle sledi da postoji vektor v koji pripada $K \cap L$. Njegova norma je

$$\|v\| = \sqrt{v_1^2 + v_2^2 + ... + v_n^2} \leq \sqrt{n} \sqrt[n]{det(L)}.$$

□

Definicija 2.2.14 (Hermitova konstanta)**.** *Ako je dato n, Hermitova konstanta γ_n je najmanja vrednost takva da nejednakost*

$$\|v\| \leq \sqrt{\gamma_n} \sqrt[n]{det(L)}.$$

važi za najkraći (ne-nula) vektor v svake rešetke L ranga n.

Na osnovu prethodne teoreme, za Hermitovu konstantu važi da je $\gamma_n \leq n$. Tačna vrednost ove konstante poznata je za $1 \leq n \leq 8$ i za $n = 24$. Vrednost $\gamma_{24} = 4$, dok su ostale vrednosti date u tabeli.

n	γ_n^n
1	1
2	$\frac{4}{3}$
3	2
4	4
5	8
6	$\frac{64}{3}$
7	64
8	256

Tabela 1: Poznate vrednosti za γ_n.

Teško je eksplicitno dati gornju granicu za dužinu najkraćeg vektora, kada je γ_n poznato samo za 9 vrednosti n. Srećom, postoje neka ograničenja kao što su

$$\frac{n}{2\pi e} \leq \gamma_n \leq \frac{n}{\pi e} \text{ i} \tag{2.20}$$

$$\gamma_n \leq \gamma_2^{n-1}, \tag{2.21}$$

za sve prirodne brojeve $n \geq 2$.

Napomena 3. *Postoje verzije Hermitove teoreme koje se odnose na više vektora. Na primer, može se pokazati da baza $v_1, v_2, ..., v_n$ rešetke L zadovoljava sledeću nejednakost*

$$\|v_1\|\|v_2\| \cdots \|v_n\| \leq \sqrt{n^n} det(L), \tag{2.22}$$

što dopunjuje Adamarovu nejednakost iz 2.7.

Definicija 2.2.15 (Adamarov odnos)**.** *Ako je data baza $v_1, v_2, ..., v_n$ rešetke $L \subset \mathbb{R}^n$, Adamarov odnos definiše se kao*

$$\mathcal{H} = \sqrt[n]{\frac{det(L)}{\|v_1\|\|v_2\| \cdots \|v_n\|}}. \tag{2.23}$$

Važi da je $0 < \mathcal{H} \leq 1$ i što je odnos bliži vrednosti 1, to su vektori u bazi više ortogonalni.

Ako je L kompletna rešetka, Gausova očekivana najkraća dužina vektora je [2]

$$o(L) = \sqrt{\frac{n}{2\pi e}} \sqrt[n]{det(L)}. \tag{2.24}$$

Gausova heuristika tvrdi da za slučajno izabranu kompletnu rešetku L, za najkraći vektor $v \in L$ važi

$$\|v\| \approx o(L).$$

2.2.1 Redukcija SVP problema na CVP problem

Piter van Emde Boas je 1981. godine takođe pokazao da je SVP problem NP-težak u ℓ_∞. Međutim, pitanje da li je problem najkraćeg vektora za ℓ_p normu, gde je $p < \infty$ NP-težak bilo je otvoreno skoro dve decenije, sve dok 1996. godine Ajtai nije pokazao da jeste, u normi ℓ_2, ali samo za nasumične redukcije. Takođe, aproksimativni problem CVP problema, tj. CVP_γ, u n-dimenzionalnoj rešetki je NP-težak za determinističke redukcije, za faktor velik kao $\gamma(n) = n^{c/\log\log n}$, $c > 0$ [7], dok se za SVP_γ problem zna da je NP-težak samo za nasumične redukcije, za faktor velik kao $\gamma(n) = 2^{(\log n)^{0.5-\varepsilon}}$, $\varepsilon > 0$ [8].
Za bilo koju normu ℓ_p, gde je $p \geq 1$, SVP problem može se redukovati na CVP, koristeći to da je CVP NP-težak. Međutim dobijaju se instance CVP-a koje su mnogo većih dimenzija nego što su dimenzije instanci originalnog SVP problema. Štaviše, NP-teškoća CVP problema ne objašnjava kako su u relaciji CVP_γ i SVP_γ kada je aproksimativni faktor polinoman ili kada norma nije ℓ_p. Zato se postavlja pitanje da li je moguće redukovati direktno SVP na CVP tako da se očuvaju dimenzije. Henk, koji je to formalizovao u [9] i kasnije Godrajh, koji je to proširio u [10], su pokazali da se SVP problem može redukovati na CVP problem u istoj dimenziji, za različite vrste normi.
Redukcija ide na sledeći način [11].
Neka je data rešetka L i njena baza $L(B) = [v_1, v_2, ..., v_m]$. Definiše se baza

$$L'(B^i) = [v_1, v_2, ..., v_{i-1}, 2v_i, v_{i+1}, ..., v_m].$$

Data baza i vektor v_i uzimaju se kao instance problema najbližeg vektora. Ove instance se prosleđuju subrutini koja rešava CVP (engl. *CVP-oracle*). Subrutina će vratiti vektore w_i, koji su najbliži vektorima v_i za $i = 1, 2, ..., n$ i pripadaju rešetki L' koja je generisana bazom $L'(B^i)$. Najkraći vektor rešetke L biće najkraći vektor u skupu $\{w_1 - v_1, ..., w_m - v_m\}$.
Dokaz za validnost njihove redukcije počinje narednom teoremom.

Teorema 2.2.5. *Neka je $L(B) = [v_1, v_2, ..., v_m]$ baza rešetke L i neka je $u = \sum_{i=1}^{m} z_i v_i$ najkraći ne-nula vektor u rešetki. Tada je bar jedno z_i neparno.*

Dokaz. Pretpostavimo da su svi $z_i, i = 1, 2, ..., m$ parni, odnosno $z_i = 2k_i, k_i \in \mathbb{Z}$. Posmatrajmo vektor

$$u' = \frac{1}{2}u = \sum_{i=1}^{m} k_i v_i.$$

Kako su k_i celi brojevi, ovaj vektor je ne-nula vektor rešetke s normom $\|u'\| = \frac{\|u\|}{2}$. Ovo je kontradikcija sa pretpostavkom da je vektor u najkraći. □

Naredna teorema nam govori da bilo koje rešenje instance SVP-a odgovara nekom rešenju jedne od CVP instanci, tačnije $(L'(B^i), v_i)$.

Teorema 2.2.6. *Neka je $L(B) = [v_1, v_2, ..., v_m]$ baza rešetke L i neka je $u = \sum_{j=1}^{m} z_j v_j$ vektor rešetke takav da je z_i neparan broj. Tada je $w = u + v_i$ vektor rešetke koja je generisana bazom $L'(B^i)$ takav da je rastojanje $d(w, v_i) = \|u\|$.*

Dokaz. Posmatrajmo vektor $w = u + v_i$. Njega možemo zapisati kao

$$w = u + v_i = \sum_{\substack{j=1 \\ j\neq i}}^{m} z_j v_j + z_i v_i + v_i = \sum_{\substack{j=1 \\ j\neq i}}^{m} z_j v_j + v_i(z_i + 1) = \sum_{\substack{j=1 \\ j\neq i}}^{m} z_j v_j + 2v_i \frac{(z_i + 1)}{2}.$$

Kako je z_i neparan, onda je $\frac{z_i+1}{2}$ ceo broj, pa je vektor w u rešetki L' čija je generatorska matrica $L'(B^i)$. Takođe, rastojanje između w i v_i je $\|w - v_i\| = \|u\|$. □

I na kraju, pokazali su da bilo koje rešenje instance $(L'(B^i), v_i)$ CVP problema odgovora ne-nula vektoru u L.

Teorema 2.2.7. *Neka je* $w = z_i(2v_i) + \sum_{\substack{j=1 \\ j\neq i}}^{m} z_j v_j$ *vektor rešetke* L' *gerenirane sa* $L'(B^i)$. *Tada je* $u = w - v_i$ *ne-nula vektor rešetke* L *generisane sa* $L(B)$.

Dokaz. Slično kao i u prethodnom dokazu, posmatramo vektor u koji je sada jednak

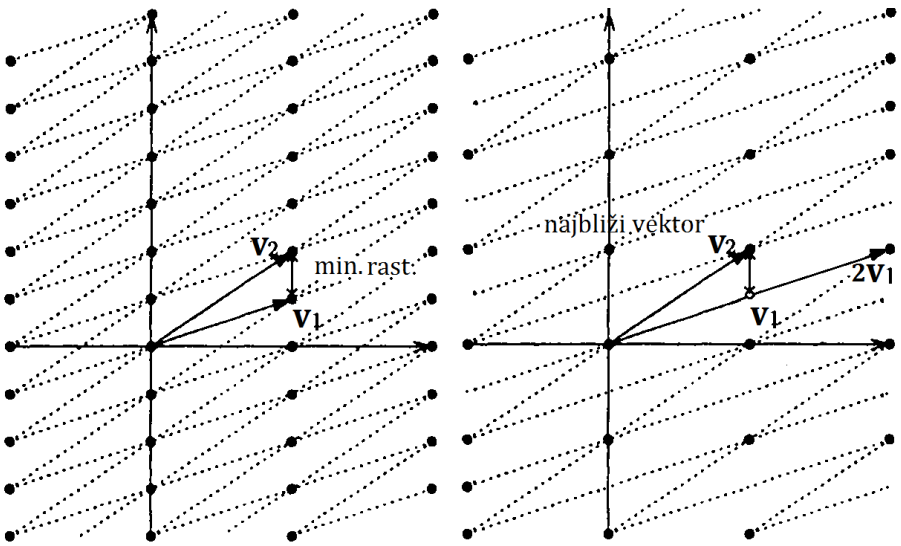
$$u = w - v_i = z_i(2v_i) + \sum_{\substack{j=1 \\ j\neq i}}^{m} z_j v_j - v_i = (2z_i - 1)v_i + \sum_{\substack{j=1 \\ j\neq i}}^{m} z_j v_j.$$

Kako je $2z_i - 1$ neparan ceo broj, različit od nule, sledi da je vektor u ne-nula vektor rešetke L. □

Neka je u najkraći ne-nula vektor rešetke L, zapisan kao linearna kombinacija baznih vektora $v_1, v_2, ..., v_m$. Na osnovu prve teoreme on mora sadržati bar jedan neparan koeficijent. Stoga, na osnovu druge teoreme, postoji instanca $(L'(B^i), v_i)$ problema najbližeg vektora čije je rešenje vektor s osobinom da mu je rastojanje od vektora v_i najviše $\|w - v_i\| = \|u\|$. Dakle, svaki najkraći vektor u rešetki L dovodi do rešenja instance $(L'(B^i), v_i)$ CVP-a, tako da je dužina vektora jednaka rastojanju između vektora mete (v_i) i tog rešenja. Sledi da među svim instancama $(L'(B^i), v_i)$ problema najbližeg vektora postoji bar jedno rešenje čije rastojanje od vektora mete ne prelazi dužinu najkraćeg vektora u rešetki L.

Treća teorema nam garantuje da svako rešenje w_i svake instance $(L'(B^i), v_i)$ daje vektor u rešetke L takav da mu je norma jednaka $\|w_i - v_i\|$. To znači da rešenja ovih instanci ne mogu imati rastojanje od svog vektora mete koje je manje od dužine najkraćeg vektora iz L.

Kombinujući ova dva rezultata dobija se da je najkraći vektor u skupu $\{w_1 - v_1, ..., w_m - v_m\}$ upravo najkraći vektor rešetke L. Dakle, SVP se može redukovati na CVP problem ovom metodom. To znači da SVP problem nije teži od CVP problema.



Slika 5: Primer redukcije u dve dimenzije.

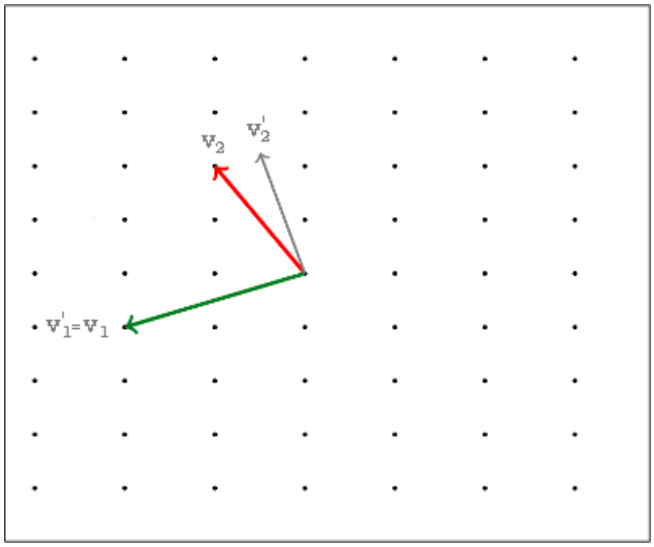
2.3 Gram-Šmitova ortogonalizacija

Gram-Šmitov (Gram-Schmidt) postupak ortogonalizacije je iterativna metoda za ortonormiranje date baze vektorskog prostora. Prvo se odabere jedan vektor i normira se. Zatim se svaki naredni vektor projektuje na ortogonalni komplement lineala prethodnih vektora i takođe se normira. U rešetkama, projekcija nekog vektora na ortogonalni komplement drugog vektora rešetke nije obavezno unutar rešetke, kao što se može videti na slici 6. Ovo znači da primena Gram-Šmitovog postupka na bazu rešetke neće uvek dati bazu koja generiše istu rešetku. Dakle, za rešetku uopšte ne mora da postoji ortogonalna (ortonormirana) baza.

Neka je data baza $v_1, v_2, ..., v_m$ rešetke L. Postupak je sledeći.

$$v_1' := v_1,$$
$$v_i' := v_i - \sum_{j=1}^{i-1} a_{ij} v_j', \quad \text{gde je } a_{ij} = \frac{\langle v_i, v_j' \rangle}{\|v_j'\|^2} \text{ za sve } 1 \leq j < i \leq m.$$

Da bi se baza ortonormirala, potrebno je još svaki vektor v_i' podeliti njegovom dužinom.



Slika 6: Postupak otgonalizacije za vektore v_1 i v_2.

Lema 2.3.1. *Ako je $v_1', v_2', ..., v_m'$ ortogonalna baza za L, onda važi jednakost*

$$det(L) = \prod_{i=1}^{m} \|v_i'\|. \tag{2.25}$$

Gram-Šmitov postupak daje različite rezultate za različit redosled vektora u bazi. Iako najčešće "novi" vektori neće biti unutar rešetke, metoda se može iskoristiti za redukciju baze u određenom smislu.

2.4 Redukcija baze rešetke

Algoritmi redukcije baze rešetke su algoritmi koji za datu bazu rešetke vraćaju novu bazu s relativno kratkim i skoro ortogonalnim vektorima. Nova baza zove se *redukovana baza*. Takva baza daje nam bolju aproksimaciju rešenja. Veliko otkriće bio je algoritam koji su 1982. izumeli Arjen Lenstra (Arjen Lenstra), Hendrik Lenstra (Hendrik Lenstra) i Laslo Lovas (László Lovász) i po njima on nosi svoj naziv *Lenstra-Lenstra-Lovász* ili tzv. LLL algoritam, koji se izvršava u polinomijalnom vremenu. Pored njega poznati su još i HKZ algoritam, Gausov i Lagranžov algoritam. LLL algoritam takođe rešava aproksimativni problem najkraćeg vektora, tako što nalazi vektor koji nije više od $(\frac{2}{\sqrt{3}})^n$ puta duži od najkraćeg vektora u rešetki, gde je n dimenzija rešetke [2].

Postupak se zasniva na ideji Gram-Šmitove ortogonalizacije i to je još jedan od razloga zašto nam je ta metoda bitna. Algoritam uzima dve baze, bazu rešetke i ortogonalnu bazu koja je dobijena Gram-Šmitovom metodom i menja ih u nekom smislu. Postupak se onda ponavlja za novodobijene baze.

Definicija 2.4.1. *LLL-redukovana baza rešetke L je uređena baza $v_1, v_2, ..., v_n$ čija Gram-Šmitova ortogonalna baza $v'_1, v'_2, ..., v'_n$ i Gram-Šmitovi koeficijenti $a_{ij} = \frac{\langle v_i, v'_j \rangle}{\|v'_j\|^2}$ zadovoljavaju:*

1. $|a_{ij}| \leq \frac{1}{2}$ *za* $1 \leq j < i \leq n$,
2. $\|v'_i\|^2 \geq (\frac{3}{4} - a_{i,i-1}^2)\|v'_{i-1}\|^2$, *za* $1 < i \leq n$.

Redukovana baza nije jedinstvena. Algoritam dakle nalazi samo jedno rešenje, od mnogih. Drugi uslov, poznat pod nazivom Lovasov (Lovászov) uslov, ekvivalentan je sa $\|v'_i + a_{i,i-1}v'_{i-1}\|^2 \geq \frac{3}{4}\|v'_{i-1}\|^2$. Ovo određuje da li je projekcija vektora v_i na ortogonalni komplement prostora $\mathcal{L}(v_1, v_2, ..., v_{i-2})$ duža od $\frac{3}{4}$ projekcije vektora v_{i-1} na ortogonalni komplement istog prostora. Ovaj uslov nam garantuje da v_i nije mnogo kraći od v_{i-1}.

Algoritam

1. Neka je $i = 1$.
2. Za svako $j = 1, 2, ..., i-1$ zameniti v_i sa $v_i - zv_j$, $z \in \mathbb{Z}$ (poželjno sa $z = 0$) tako da svaki novi Gram-Šmitov koeficijent a_{ij} zadovoljava $|a_{ij}| \leq \frac{1}{2}$.
3. Dalje raditi sledeće:
   - Ako je Lovasov uslov zadovoljen i $i = n$, stati.
   - Ako je Lovasov uslov zadovoljen i $i < n$, povećati i i vratiti se na korak 2.
   - Ako Lovasov uslov nije zadovoljen, zameniti v_i sa v_{i-1}, smanjiti i i vratiti se na korak 2.

Primer 2.4.1. [12] Neka je data baza $(1, 1, 1), (-1, 0, 2), (3, 5, 6)$ trodimenzionalne rešetke $L \subset \mathbb{R}^3$. Njena odgovarajuća generatorska matrica je

$$L(B) = \begin{bmatrix} 1 & -1 & 3 \\ 1 & 0 & 5 \\ 1 & 2 & 6 \end{bmatrix}.$$

1. Neka je $i = 1$.
   $v_1' = v_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ $\langle v_1', v_1' \rangle = \langle \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \rangle = 3$

2. Za $i = 2$ raditi sledeće:
   Za $j = 1$ računa se Gram-Šmitov koeficijent
   $a_{2,1} = \frac{\langle v_2, v_1' \rangle}{\langle v_1', v_1' \rangle} = \langle \begin{bmatrix} -1 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \rangle / 3 = \frac{1}{3}$, što je manje od $\frac{1}{2}$, pa se ne mora vršiti zamena.

3. U ovom koraku se proverava da li je Lovasov uslov zadovoljen.
   Računa se $v_2' = v_2 - a_{2,1} v_1' = \begin{bmatrix} -1 \\ 0 \\ 2 \end{bmatrix} - \frac{1}{3} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} -4/3 \\ -1/3 \\ 5/3 \end{bmatrix}$. Odatle sledi da je $\langle v_2', v_2' \rangle = \langle \begin{bmatrix} -4/3 \\ -1/3 \\ 5/3 \end{bmatrix}, \begin{bmatrix} -4/3 \\ -1/3 \\ 5/3 \end{bmatrix} \rangle = \frac{14}{3}$.
   $\|v_2' + a_{2,1} v_1'\|^2 = \| \begin{bmatrix} -4/3 \\ -1/3 \\ 5/3 \end{bmatrix} + \frac{1}{3} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \|^2 = 5 > \frac{9}{4} = \frac{3}{4} \|v_1'\|^2$
   Dakle, uslov jeste zadovoljen i pošto je $i < n$, i se povećava za 1 i ponavlja se korak 2.

2. Sada je $i = 3$.

   - Za $j = 1$ računa se Gram-Šmitov koeficijent
     $a_{3,1} = \frac{\langle v_3, v_1' \rangle}{\langle v_1', v_1' \rangle} = \langle \begin{bmatrix} 3 \\ 5 \\ 6 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \rangle / 3 = \frac{14}{3} > \frac{1}{2}$
     Sada se zamenjuje v_3 sa $v_3 - z v_1$. Za ceo broj z često se uzima $z = \lfloor 0.5 + a_{i,j} \rfloor$, što će i ovde biti učinjeno.
     $v_3 = v_3 - \lfloor 0.5 + a_{3,1} \rfloor v_1 = \begin{bmatrix} 3 \\ 5 \\ 6 \end{bmatrix} - 5 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} -2 \\ 0 \\ 1 \end{bmatrix}$
     $a_{3,1} = \langle \begin{bmatrix} -2 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \rangle / 3 = -\frac{1}{3} < \frac{1}{2}$
     Novo $a_{3,1}$ se može računati i kao $a_{3,1} = a_{3,1} - z$.
   - Sada se isti postupak ponavlja za $j = 2$.
     $a_{3,2} = \frac{\langle v_3, v_2' \rangle}{\langle v_2', v_2' \rangle} = \langle \begin{bmatrix} 3 \\ 5 \\ 6 \end{bmatrix}, \begin{bmatrix} -4/3 \\ -1/3 \\ 5/3 \end{bmatrix} \rangle / \frac{14}{3} = \frac{13}{14} > \frac{1}{2}$
     $v_3 = v_3 - \lfloor 0.5 + a_{3,2} \rfloor v_2 = \begin{bmatrix} 3 \\ 5 \\ 6 \end{bmatrix} - \begin{bmatrix} -1 \\ 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \\ 4 \end{bmatrix}$
     Gram-Šmitov koeficijent je sada $a_{3,2} = a_{3,2} - 1 = \frac{13}{14} - 1 = -\frac{1}{14} < \frac{1}{2}$.
     Dakle, nova matrica je

$$L(B) = \begin{bmatrix} 1 & -1 & 4 \\ 1 & 0 & 5 \\ 1 & 2 & 4 \end{bmatrix}.$$

3. Dalje se proverava da li je zadovoljen Lovasov uslov.
   Prvo treba izračunati v_3'. $v_3' = v_3 - a_{3,1}v_1' - a_{3,2}v_2' = \begin{bmatrix} 3 \\ 5 \\ 6 \end{bmatrix} - \frac{14}{3}\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} - \frac{13}{14}\begin{bmatrix} -4/3 \\ -1/3 \\ 5/3 \end{bmatrix} = \begin{bmatrix} -5/3 \\ 1/3 \\ 4/3 \end{bmatrix} - \frac{13}{14}\begin{bmatrix} -4/3 \\ -1/3 \\ 5/3 \end{bmatrix} = \begin{bmatrix} -6/14 \\ 9/14 \\ -3/4 \end{bmatrix}$, te je $\langle v_3', v_3' \rangle = \frac{9}{14}$.

   Lovasov uslov sada nije zadovoljen, jer je $\frac{9}{14} \approx 0.643 < 3.478 \approx (\frac{3}{4} - (-\frac{1}{14})^2)\frac{14}{3}$.
   Dakle, moramo zameniti v_3 sa v_2, smanjiti i na 2 i ponoviti korak 2.

Sada se dobija nova matrica

$$L(B) = \begin{bmatrix} 1 & 4 & -1 \\ 1 & 5 & 0 \\ 1 & 4 & 2 \end{bmatrix}.$$

2. $a_{2,1} = \frac{\langle v_2, v_1' \rangle}{\langle v_1', v_1' \rangle} = \langle \begin{bmatrix} 4 \\ 5 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \rangle / 3 = \frac{13}{3} > \frac{1}{2}$

   Zamenjuje se v_2 sa $v_2 - \lfloor 0.5 + a_{2,1} \rfloor v_1 = \begin{bmatrix} 4 \\ 5 \\ 4 \end{bmatrix} - \begin{bmatrix} 4 \\ 4 \\ 4 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$.
   Sada je $a_{2,1} = a_{2,1} - 4a_{1,1} = \frac{13}{4} - 4 = \frac{1}{3} < \frac{1}{2}$.

3. Lovasov uslov opet nije zadovoljen, jer je
   $\langle v_2', v_2' \rangle = \frac{2}{3} < \frac{23}{12} = (\frac{3}{4} - (\frac{1}{3})^2)3 = (\frac{3}{4} - a_{2,1}^2)\langle v_1', v_1' \rangle$ To znači da se zamenjuje v_2 i v_1.

Krajnja, LLL-redukovana baza je

$$L(B) = \begin{bmatrix} 0 & 1 & -1 \\ 1 & 1 & 0 \\ 0 & 1 & 2 \end{bmatrix}.$$

Važno svojstvo LLL-redukovane baze je da je prvi vektor relativno kratak.

Teorema 2.4.1. *Neka je $v_1, v_2, ..., v_n$ LLL-redukovana baza rešetke $L \subset \mathbb{R}^n$. Tada je*

$$\|v_1\| \leq 2^{(\frac{n-1}{2})}\|v\|,$$

za svako $v \in L$.

Dokaz. Za bilo koji vektor rešetke važi $\|v\| \geq \min_i \|v_i'\|$, gde je $v_1', v_2', ..., v_n'$ Gram-Šmitova ortogonalna baza za redukovanu bazu. S druge strane je

$$\|v_n'\|^2 \geq \frac{1}{2}\|v_{n-1}'\|^2 \geq \cdots \geq (\frac{1}{2})^{n-1}\|v_1'\|^2 = (\frac{1}{2})^{n-1}\|v_1\|^2.$$

Odatle sledi da za svako i važi

$$\|v_1\| = \|v_1'\| \leq (\frac{1}{2})^{-\frac{(i-1)}{2}}\|v_i'\| \leq (\frac{1}{2})^{-\frac{(n-1)}{2}}\|v_i'\|.$$

Dakle,

$$\|v_1\| \leq (\frac{1}{2})^{-\frac{(n-1)}{2}} \min_i \|v_i'\| \leq (\frac{1}{2})^{-\frac{(n-1)}{2}}\|v\|,$$

što je i trebalo pokazati. □

2.5 Babaijev algoritam

Pored toga što je moguće koristiti algoritme redukcije baze za rešavanje aproksimativnog problema najkraćeg vektora, to je moguće učiniti i za aproksimativni problem najbližeg vektora. Laslo Babai[3] (László Babai) je 1986. godine objavio dve metode za rešavanje CVP_γ problema, metodu zaokruživanja i algoritam najbliže ravni. Prvi korak oba algoritma je primena LLL algoritma, kako bi se smanjila dužina baznih vektora i povećala njihova međusobna ortogonalnost. Algoritam najbliže ravni daje bolji aproksimativni faktor, dok je algoritam zaokruživanja jednostavniji.
Neka je $L \subset \mathbb{R}^n$ kompletna rešetka, s redukovanom bazom $v_1, v_2, ..., v_n$. Ako je $w \in \mathbb{R}^n$ vektor za koji tražimo najbliži u rešetki, onda se on može napisati kao linearna kombinacija baznih vektora

$$w = \sum_{i=1}^{n} t_i v_i, \quad t_i \in \mathbb{R}.$$

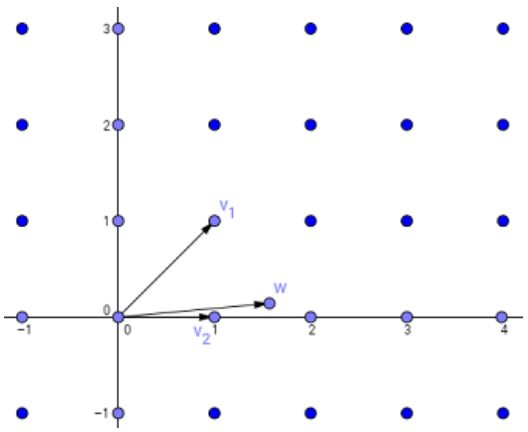
Zatim se svaki koeficijent t_i zaokruži na najbliži ceo broj $\lfloor t_i \rceil$. Rezultujući vektor v je linearna kombinacija baznih vektora s koeficijentima $\lfloor t_i \rceil$.

Algoritam

1. Napisati w kao $w = t_1 v_1 + t_2 v_2 + ... + t_n v_n$, $t_i \in \mathbb{R}$, za $i = 1, 2, ..., n$.
2. Neka je $a_i = \lfloor t_i \rceil$ za $i = 1, 2, ..., n$.
3. Izračunati izlazni vektor $v = a_1 v_1 + a_2 v_2 + ... + a_n v_n$.

Babai je pokazao da metoda zaokruživanja nalazi približno rešenje za CVP_γ sa aproksimativnim faktorom $\gamma(n) = 1 + 2n(\frac{9}{2})^{n/2}$.

Primer 2.5.1. Neka je $L = \mathbb{Z}^2$. Ako se uzme "loša" baza kao ulaz za algoritam, ne dobija se dobro rešenje. Neka je baza $v_1 = (1, 1)$, $v_2 = (1, 0)$, a vektor meta $w = (\frac{11}{7}, \frac{1}{7})$. Kada se w izrazi kao linearna kombinacija baznih vektora dobija se $w = \frac{1}{7}v_1 + \frac{10}{7}v_2$. Posle zaokruživanja koeficijenata, ovo postaje $w = v_2 = (1, 0)$. Međutim, vektor koji je najbliži datom vektoru je $2v_2 = (2, 0)$.



Slika 7: Primer Babaijeve metode zaokruživanja

[3]Laslo Babai, rođen 20.7.1950. u Mađarskoj, profesor je računarstva i matematike na Univerzitetu u Čikagu.

3 Neki kriptosistemi zasnovani na rešetkama

U ovoj glavi biće predstaviljena tri najpoznatija kriptosistema zasnovana na rešetkama - Ajtai Dvork (Ajtai-Dwork), Goldrajh-Goldvaser-Halevi (Goldreich-Goldwasser-Halevi) ili skraćeno GGH i NTRU kriptosistem.

Definicija 3.0.1. *Kriptosistem je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju važi:*

- $\mathcal{P}$ *je konačan skup svih mogućih osnovnih elemenata otvorenog teksta;*
- $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata;*
- $\mathcal{K}$ *je prostor ključeva, tj. konačan skup svih mogućih ključeva;*
- *Za svaki ključ* $k \in \mathcal{K}$ *postoji funkcija šifrovanja* $e_k \in \mathcal{E}$ *i odgovarajuća funkcija dešifrovanja* $d_k \in \mathcal{D}$. *Pritom su* $e_k : \mathcal{P} \to \mathcal{C}$ *i* $d_k : \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da je* $d_k(e_k(x)) = x$ *za svaki otvoreni tekst* $x \in \mathcal{P}$.

3.1 Ajtai-Dvork kriptosistem

Miklos Ajtai i Sintija Dvork[4] (Cynthia Dwork) su izumeli ovaj kriptosistem 1997. godine. Ono što je interesantno je to da su oni pokazali da je ovaj sistem dokazivo siguran, osim ako se najteži slučaj problema jedinstvenog najkraćeg vektora (uSVP$_\gamma$) u rešetki može rešiti u polinomnom vremenu za neki polinom $\gamma \approx n^8$. Iako ga oni nisu prezentovali koristeći rešetke, dokaz o sigurnosti je pokazao da se svaka instanca problema jedinstvenog najkraćeg vektora može s velikom verovatnoćom transformisati u nasumičnu instancu njihovog kriptosistema. Nažalost, u odnosu na ostale kriptosisteme s javnim ključem, ovaj kriptosistem nije toliko efikasan. Detaljnijom kriptoanalizom i eksperimentima, pokazano je da ako bismo želeli sigurnost, implementacija Ajtai-Dvork kriptosistema bi zahtevala veoma dugačke ključeve, što nije praktično. Pre nego što je počeo da radi na kriptosistemu, Ajtai je u svom radu "Generating hard instances of lattice problems" [4] predstavio povezanost između najtežeg i prosečnog slučaja kompleksnosti SVP problema, pokazavši da se svaka instanca najtežeg slučaja može redukovati na neku nasumičnu instancu prosečnog slučaja. Kao što je prethodno spomenuto, on je dokazao da je SVP NP-težak u normi ℓ_2 za nasumične redukcije [13]. U dokazu je koristio redukciju da transformiše instance problema jedinstvenog najkraćeg vektora u aproksimativni SVP problem za nasumičnu instancu specijalne klase rešetke. Ovo znači da je prosečan slučaj težak bar onoliko koliko je najteži slučaj, što je vrlo željeno svojstvo za kriptosisteme.

Ajtaijeva heš funkcija

Neka je dat parametar n. Slučajno se bira matrica dimenzije $n \times m$ čiji su elementi iz skupa $\mathbb{Z}_q = \{0, 1, ..., q-1\}$, gde je q velik prost broj, a m i q odabrani tako da je $n \log_2 q < m < q/2n^4$ i $q = \mathcal{O}(n^k)$, za neki ceo broj $k > 0$. Heš funkcija h_M preslikava nizove bitova dužine m u skup $\mathbb{Z}_q^n$, odnosno

$$h_M : \ \{0,1\}^m \to \mathbb{Z}_q^n.$$

Ako je $s = s_1 s_2 ... s_m$ string iz skupa $\{0,1\}^m$, onda je ovo preslikavanje definisano sa

$$h_M(s) = R_q[Ms] = R_q\Big[\sum_{i=1}^{m} s_i M_i\Big], \tag{3.1}$$

gde je M_i i-ta kolona matrice M. S obzirom na to da funkcija uzima elemente dužine m i slika ih u elemente dužine $n \log_2 q$ (u bitovima), a $m > n \log_2 q$, to znači da će doći do nekih preklapanja,

[4] Sintia Dvork je američka naučnica, rođena 1958. godine, zaposlena u Majkrosoft istraživačkom centru.

tj. kolizija. Ajtai je međutim pokazao da je nemoguće naći ove kolizije, sem ako se ne zna dobra aproksimacija rešenja najtežeg slučaja uSVP$_\gamma$ problema u rešetki.
Ajtai je u svom radu opisao naredni problem, koji se odnosi na heš funkciju iz 3.1: Za parametre n, m, q koji zadovoljavaju gore navedene uslove i matricu M sa elementima iz skupa $\mathbb{Z}_q$ treba naći vektor $x \in \mathbb{Z}_q^m$ za koji važi $\|x\| < n$ i $R_q[Mx] = 0$.

Ajtai-Dvork kriptosistem.
Neka je h_M heš funkcija s parametrima n, m, q i matricom M. Za jednosmernu funkciju sa zamkom Ajtai je predložio funkciju

$$f(M, s) = (M, h_M(s)),$$

gde je s niz (string) bitova. Zamka se zasniva na rešivosti problema najkraćeg vektora za dobru bazu rešetke.
Neka je dat sigurnosni parametar n, koji određuje dimenziju vektorskog prostora kao i rešetke. Dalje, neka je $v_1, v_2, ..., v_m$ baza rešetke, gde je $m = n^3$. Kocka u $\mathbb{R}^n$, centralizovana u nuli, s ivicom dužine $a_n = 2^{n \log_2 n} = n^n$ data je skupom

$$K_n = \{x \in \mathbb{R}^n | \ |x_i| \leq a_n/2, \forall i\}. \tag{3.2}$$

Zatvorena lopta u $\mathbb{R}^n$ s centrom u nuli, poluprečnika n^{-k}, za ceo broj $k > 0$ (u originalnom papiru uzeto je $k = 8$) je

$$B_n = \{x \in \mathbb{R}^n | \ \|x\| \leq n^{-k}\}. \tag{3.3}$$

Tajni ključ je vektor p koji se bira nasumično iz $n-$dimenzionalne jedinične lopte. Tada je raspodela $\mathcal{F}_p$ definisana na K_n data sa:

- Slučajno i uniformno birati vektor x iz skupa $\{x \in K_n | \ \langle x, p\rangle \in \mathbb{Z}\}$.
- Uzeti nezavisno n vektora $y_1, y_2, ..., y_n$ iz skupa B_n, takođe uniformno i nasumično.
- Izlaz je vektor $v = x + y_1 + ... + y_n$.

Javni ključ dobija se tako što se vektori $w_1, w_2, ..., w_n, v_1, v_2, ..., v_m$ biraju slučajno, raspodelom $\mathcal{F}_p$. Vektori $w_1, w_2, ..., w_n$ moraju da zadovoljavaju uslov da fundamentalni paralelopiped kojeg generišu nije previše pljosnat. To znači da minimalna udaljenost vektora w_i i hiperravni koja je određena preostalim vektorima mora da bude najmanje a_n/n^2 za sve $i = 1, 2, ..., n$. Sve dok ovaj uslov nije ispunjen generiše se novi ključ. Takođe, vektor v može biti redukovan po modulu paralelopipeda tako što se nađe vektor v' takav da je razlika $v - v'$ vektor rešetke generisane vektorima w_i. Ovo se zapisuje kao $v' = R_{\mathcal{F}}[v]$.

Šifrovanje se odvija bit po bit, odnosno svaki bit se posebno šifruje.

- Da bi se šifrovala 0, $s_1, s_2, ..., s_m$ biraju se uniformno i nasumično iz skupa $\{0, 1\}$ i redukuje se vektor $\sum_{i=1}^{m} s_i v_i$ po modulu paralelopipeda $\mathcal{F}(w_1, w_2, ..., w_n)$. Dobijeni $n-$dimenzionalni vektor biće upravo šifrovani tekst.
- Da bi se šifrovala 1, nasumično se bira $n-$dimenzionalni vektor paralelopipeda $\mathcal{F}(w_1, w_2, ..., w_n)$ i to je šifrovani tekst.

Dešifrovanje datog šifrovanog teksta c, odnosno $n-$dimenzionalnog vektora koji odgovara jednom bitu otvorenog teksta veoma je jednostavno. Prvo se izračuna skalarni proizvod $\langle c, p\rangle$. Ako je rastojanje $d(\langle c, p\rangle, \mathbb{Z}) \leq n^{-1}$, onda je se c dešifruje kao 0, inače kao 1.

Lema 3.1.1. *Šifrat nule će uvek biti dešifrovan kao nula, dok će šifrat jedinice sa verovatnoćom $\frac{2}{n}$ biti dešifrovan kao nula.*

Dokaz. Neka je c šifrovana 0, odnosno $c = R_{\mathcal{F}}\Big[\sum_{i=1}^{m} s_i v_i\Big]$, $\mathcal{F} = \mathcal{F}(w_1, w_2, ..., w_n)$ i neka je za svaki v_i skalarni proizvod $\langle v_i, p\rangle \in \mathbb{Z} \pm n^{-k}$, gde je $k = 8$. Dakle, $\sum_{i=1}^{m=n^3} s_i v_i \in \mathbb{Z} \pm n^{3-k}$. Odavde sledi da je $c = \sum_{i=1}^{m} s_i v_i + \sum_{i=1}^{n} a_i w_i$, gde je $a_i < n^4$, pa $c \in \mathbb{Z} \pm n^{-1}$. Posmatrajmo sada slučaj kada je c enkripcija jedinice. Ovo znači da je vektor $c \in \mathcal{F}(w_1, w_2, ..., w_n)$ biran uniformno i nasumično. Uzmimo da je $t := \langle c, p\rangle - \lfloor\langle c, p\rangle\rfloor$. Kako je c birano uniformno i nasumično, onda je i ovo uniformno na skupu $[0, 1]$. Ako je $t < n^{-1}$ ili $t > 1 - n^{-1}$, c se dešifruje kao nula. Dakle, verovatnoća da se c dešifruje kao nula je tačno $2n^{-1} = \frac{2}{n}$. □

Glavni rezultat je da verovatnosni algoritam koji razlikuje enkripciju 0 od enkripcije 1 sa nekom polinomnom prednošću može biti korišćen za nalaženje najkraćeg ne-nula vektora u bilo kojoj n-dimenzionalnoj rešetki, gde je taj najkraći vektor jedinstven. Tačnije, Ajtai i Dvork su pokazali da ako se enkripcija 0 može razlikovati od enkripcije 1 u polinomijalnom vremenu bez poznavanja tajnog ključa, sa verovatnoćom n^{-k}, onda najteži slučaj problema jedinstvenog najkraćeg vektora ima verovatnosno rešenje u polinomijalnom vremenu.

Praktični aspekat kriptosistema

Tajni ključ je vektor u $n-$dimenzionaloj jediničnoj lopti, a pošto je binarno širenje svakog ulaza n, tajni ključ zahteva n^2 bitova u prostoru. Javni ključ se pak sastoji od $n + n^3$ $n-$dimenzionalnih vektora s elementima veličine $\pm a_n/2 = \pm n^n/2$, što zahteva najmanje $n^3 n \log_2 n^n = n^5 \log_2 n$ bita. Kako je šifrat jednog bita u stvari vektor unutar fundamentalnog paralelopipeda, onda je šifrat $n-$dimenazionalni vektor čije koordinate pripadaju $[-a_n/2, a_n/2]$. Kao i malopre, ako uzmemo u obzir da je binarno širenje n, onda se šifrat može predstaviti kao $n(\log_2(n^n) + n) = n^2(\log_2 n + 1)$ bita.

Objekat	Veličina u bitovima
Tajni ključ	n^2
Javni ključ	$n^5 \log_2 n$
Šifrovani tekst	$n^2(\log_2 n + 1)$

Tabela 2: Veličine ključeva i šifrovanog teksta u AD kriptosistemu.

3.2 GGH kriptosistem

GGH kritosistem objavljen je 1997. godine. Izumeli su ga Oded Goldrajh (Oded Goldreich), Šafi Goldvaser (Shafi Goldwasser) i Šai Halevi (Shai Halevi). Za razliku od prethodnog kriptosistema, ovaj kriptosistem se zasniva na problemu najbližeg vektora i znatno je efikasniji.

Enkripcija

Neka su Filip i Tanja dvoje ljudi koji žele bezbedno da komuniciraju. Tanja, kao tajni ključ, bira skup od n linearno nezavisnih vektora $v_1, v_2, ..., v_n \in \mathbb{Z}^n$, koji su relativno kratki i skoro ortogonalni, dakle tajni ključ je dobra baza rešetke $L \subseteq \mathbb{Z}^n$. Jedan od načina da Tanja ovo uradi je da fiksira parametar k i zatim bira koordinate ovih vektora nasumično između $-k$ i k. Tanja može da proveri da je zaista dobila dobru bazu, računajući Adamarov odnos. Ako on nije previše mali, baza je dobra. Dalje, ona bira unimodularnu matricu U, dimenzije $n \times n$. Zatim računa ekvivalentnu bazu, tačnije njenu odgovarajuću generatorsku matricu $B' = L(B)U$, gde se matrica U može dobiti na više načina, kao na primer množenjem velikog broja elementarnih matrica. Vektori kolona ove matrice, $b_1, b_2, ..., b_n$, su Tanjin javni ključ.

Ako Filip želi da pošalje poruku Tanji, on treba da izabere mali vektor m kao njegov otvoreni tekst. To može biti binarni vektor. On takođe nasumično bira (mali) vektor "smetnje" s, koji se ponaša kao privremen ključ. Koordinate ovog vektora Filip može na primer da bira nasumično između $-\varepsilon$ i ε, gde je ε neki fiksiran javni parametar (sigurnosni parametar). On zatim računa vektor

$$c = B'm + s = \sum_{i=1}^{n} m_i b_i + s_i, \tag{3.4}$$

koji će predstavljati šifrat. Ovaj vektor nije u rešetki, ali je veoma blizu vektora $B'm$ koji jeste u rešetki, s obzirom na to da je vektor smetnje mali.

Dekripcija

Da bi dešifrovala c, Tanja koristi Babaijev algoritam za bazu $v_1, v_2, ..., v_n$ kako bi našla vektor u rešetki koji je blizu vektora c. Pošto ona koristi dobru bazu i vektor smetnje s je mali, vektor rešetke koji ona nalazi je $B'm$. Nakon toga ona, množeći taj vektor sleva sa $(B')^{-1}$, dobija traženi vektor m.

Napomena 4. *Daniele Mićanco (Daniele Micciancio) je predložio da se matrica B' računa kao Hermitova normalna forma (HNF) matrice $L(B)$, radi veće efikasnosti (za više pogledati [14]).*

Primer 3.2.1. [15] Neka je dimenzija rešetke $n = 4$, a sigurnosni parametar $\varepsilon = 1$. Matrica $L(B)$ koja je tajni ključ generiše se nasumično tako da su njeni elementi celi brojevi između -4 i 4 (metoda koja je predloženo u [16]). Neka je javna matrica B' Hermitova normalna forma matrice $L(B)$ kao što je implementirano u programu *Mathematica*[5]. Rezultujuće matrice su

$$L(B) = \begin{bmatrix} 3 & 1 & -1 & 3 \\ 3 & -4 & 3 & 1 \\ 3 & -3 & -4 & -3 \\ -2 & -3 & -2 & 3 \end{bmatrix} \quad B' = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 \\ -349 & 311 & 321 & 851 \end{bmatrix}$$

Može se proveriti da li je generatorska matrica dobra baza rešetke L, tako što se izračuna Adamarov odnos

$$\mathcal{H} = \sqrt[4]{\frac{det(L)}{\|v_1\|\|v_2\|\|v_3\|\|v_4\|}} \approx \sqrt[4]{\frac{851}{954.673}} \approx \frac{5.4011}{5.55857} \approx 0.97.$$

[5]Implementacija Hermitove normalne forme u programu *Mathematica* se razlikuje od standardne implementacije. Iako dobijena matrica nije baš pogodna za enkripciju, ne utiče na ovaj primer.

Adamarov odnos je vrlo blizu jedinici, što znači da je izbor baze dobar. Dalje, neka je $m = (-2, 0, -4, -1)^T$ poruka koju želimo da šifrujemo koristeći vektor smetnje $s = (-1, 1, 1, -1)^T$. Šifrat c dat je sa

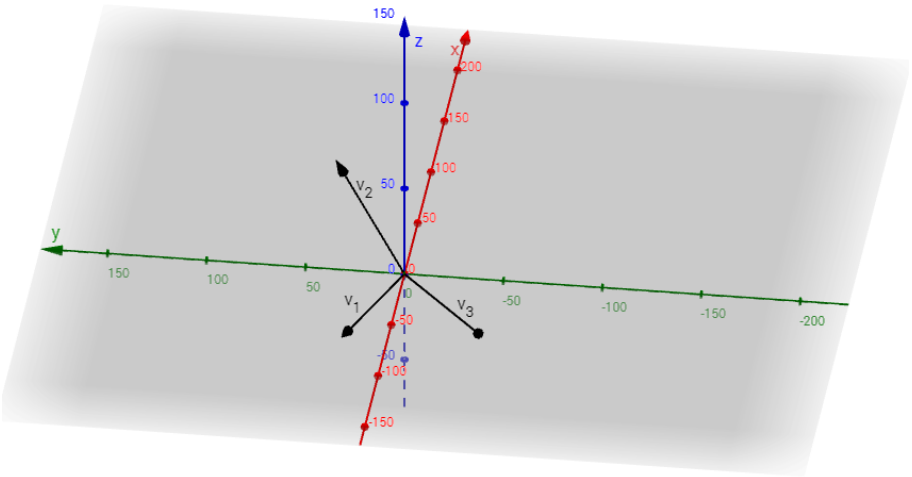
$$c = B'm + s = (-3, 1, -3, -1438).$$

Da bismo dešifrovali poruku c koristimo prvo Babaijev algoritam, gde dobijamo vektor u rešetki koji je najbliži vektoru $B'm+s$, a to je $B'm = (-2, 0, -4, -1437)$, pa još množeći sleva matricom $(B')^{-1}$ dobijamo poruku $m = (-2, 0, -4, -1)$.

Primer 3.2.2. [2] Neka je $L \subset \mathbb{Z}^3$ trodimenzionalna rešetka, a njena dobra baza, odnosno tajni ključ, $v_1 = (-97, 19, 19)^T$, $v_2 = (-36, 30, 86)^T$ i $v_3 = (-184, -64, 78)^T$. Proverimo da li je ovo zaista dobra baza za rešetku.
Adamarov odnos je

$$\mathcal{H} = \sqrt[3]{\frac{det(L)}{\|v_1\|\|v_2\|\|v_3\|}} \approx 0.74620.$$

Pošto je ovaj broj dovoljno blizu jedinice, baza je dobro izabrana. Možemo se u to uveriti i ilustracijom datih vektora.



Slika 8: Dobra (tajna) baza rešetke L.

Dalje računamo $B' = L(B)U$, odnosno

$$\begin{bmatrix} -97 & -36 & -184 \\ 19 & 30 & -64 \\ 19 & 86 & 78 \end{bmatrix} \begin{bmatrix} 4327 & 3297 & 5464 \\ -15447 & -11770 & -19506 \\ 23454 & 17871 & 29617 \end{bmatrix},$$

gde je matrica U dobijena množenjem velikog broja elementarnih matrica. Njena determinanta je -1. Dobijamo matricu

$$B' = \begin{bmatrix} -4179163 & -3184353 & -5277320 \\ -1882253 & -1434201 & -2376852 \\ 583183 & 444361 & 736426 \end{bmatrix}.$$

Dakle, vektori javne (loše) baze su

$$w_1 = (-4179163, -1882253, 583183)^T,$$

$$w_2 = (-3184353, -1434201, 444361)^T,$$

$$w_3 = (-5277320, -2376852, 736426)^T.$$

Adamarov odnos,

$$\mathcal{H} = \sqrt[3]{\frac{det(L)}{\|w_1\|\|w_2\|\|w_3\|}} \approx 0.0000208,$$

je zaista veoma mali.
Ako želimo da pošaljemo otvoreni tekst $m = (86, -35, -32)^T$ koristeći vektor smetnje $s = (-4, -3, 2)^T$, onda je odgovarajući šifrat

$$c = B'm + s = \begin{bmatrix} -4179163 & -3184353 & -5277320 \\ -1882253 & -1434201 & -2376852 \\ 583183 & 444361 & 736426 \end{bmatrix} \begin{bmatrix} 86 \\ -35 \\ -32 \end{bmatrix} + \begin{bmatrix} -4 \\ -3 \\ 2 \end{bmatrix} = \begin{bmatrix} -79081427 \\ -35617462 \\ 11035473 \end{bmatrix}.$$

Da bi primalac dešifrovao poruku m, prvo mora da primeni Babaijev algoritam. On zapisuje vektor c kao linearnu kombinaciju vektora tajne baze s realnim koeficijentima

$$c \approx 81878.97v_1 - 292300v_2 + 443815v_3,$$

a zatim zaokružuje ove koeficijente na najbliže cele brojeve kako bi dobio vektor rešetke

$$v = 81879v_1 - 292300v_2 + 443815v_3 = (-79081423, -35617459, 11035471)^T$$

koji je najbliži vektoru c. Sada vektor m računa tako što napiše vektor v kao linearnu kombinaciju vektora javne baze, odnosno

$$v = 86w_1 - 35w_2 - 32w_1.$$

Vektor m čine upravo koeficijenti uz w_1, w_2 i w_3.
Pretpostavimo da napadač želi da pročita ovu poruku. Njemu je poznata loša baza rešetke B'. Ako on primeni Babaijevu metodu na ovu bazu, vektor koji nalazi je

$$c \approx 75.76w_1 - 34.52w_2 - 24.18w_3.$$

Nakon zaokruživanja koeficijenata dobija vektor rešetke

$$w = 75w_1 - 35w_2 - 24w_3 = (-79508353, -35809745, 11095049)^T.$$

Ovaj vektor, iako jeste donekle blizu vektora c, daje pogrešan otvoreni tekst $m = (76, -35, -24)^T$. Ako uporedimo rastojanja vektora v i w od vektora c

$$\|c - v\| \approx 5.3852 \text{ i } \|c - w\| \approx 472000,$$

vidimo koliko je vektor v zaista bliži vektoru c, što pokazuje koliko Babaiev algoritam dobro radi ako je baza dobro izabrana.

Praktični aspekat kriptosistema

Neka je $L \subseteq \mathbb{Z}^n$ kompletna rešetka. Tajni ključ, odnosno matrica $L(B)$ sadrži n^2 celih brojeva, što zahteva $n^2 \log_2 k$ bita u prostoru, gde su elementi matrice iz intervala $[i, i+k]$, $i \in \mathbb{Z}$. Daniele Mićanco[6] pokazao je u [17] da ako je svejedno na koji način je matrica B' dobijena od matrice $L(B)$, javni ključ B' može da postane matrica dimenzije $n \times n$ sa celobrojnim elementima čija reprezentacija zahteva $O(n \log_2 n)$ bitova. Ovo znači da javni ključ zahteva $O(n^3 \log_2 n)$ bitova u prostoru. Ako se matrica B' dobija kao Hermitova normalna forma, onda to može da se redukuje na $O(n^2 \log_2 n)$ bita. Šifrovanje pak zahteva množenje matrice $n \times n$ sa vektorom dimenzije n kao i sabiranje sa vektorom iste dimenzije, a za to je potrebno vreme $O(n^2 \log_2 n)$.

Objekat	**Veličina u bitovima**
Tajni ključ	$n^2 \log_2 k$
Javni ključ	$n^2 \log_2 n$
Operacija	**Vreme**
Šifrovanje	$n^2 \log_2 n$

Tabela 3: Veličine ključeva i vreme šifrovanja u GGH kriptosistemu.

Dakle, ako je na primer $n = 400$, onda bi tajni kluč bila matrica dimenzije 400×400, što je 160.000 elemenata. To je vrlo nepraktično, te ovaj kriptosistem ima više teorijski značaj, kao motivacija za konstruisanje nekog praktičnijeg sistema.

[6]Daniele Mićanco je profesor računarstva i automatike na Univerzitetu u San Dijegu, član odseka za kriptografiju i sigurnost.

3.3 NTRU kriptosistem

Prvu verziju ovog asimetričnog kriptosistema predstavili su Džefri Hofsten (Jeffrey Hoffstein), Džil Pifer (Jill Pipher) i Džozef Silverman (Joseph Silverman) 1996. godine u [18]. NTRU (engl. *N-th degree TRUncated polinomial ring*) je kriptosistem koji se opisuje kao kriptosistem prstena polinoma. Zasniva se na problemu najkraćeg vektora. NTRU se u stvari sastoji od kriptosistema NTRUEncrypt i šeme digitalnog potpisa NTRUSign. Ovde će biti opisan kriptosistem, a pre nego što to bude učinjeno treba se podsetiti nekih algebarskih struktura.

3.3.1 Konvolucijski prsten polinoma

Definicija 3.3.1 (Prsten)**.** *Strukturu* $(R, +, \cdot)$ *gde je* R *neprazan skup zovemo prsten ukoliko je za binarne operacije* $+ : R \times R \to R$ *i* $\cdot : R \times R \to R$*, ispunjeno sledeće:*

$(R, +)$ *je Abelova grupa s neutralnim elementom* 0*:*

- *Za svako* a *i* b *iz* R*,* $a + b$ *je takođe u* R*;*
- $(a + b) + c = a + (b + c)$*;*
- $0 + a = a + 0 = a$*;*
- $a + b = b + a$*;*
- *Za svako* a *iz* R*, postoji inverzni element koji se označava sa* $-a$*, takav da važi* $a + (-a) = (-a) + a = 0$*.*

$(R, \cdot)$ *je polugrupa, odnosno važi:*

- *Za svako* a *i* b *iz* R*,* $a \cdot b$ *takođe pripada* R*;*
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*.*

Množenje je distributivno u odnosu na sabiranje:

- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$*;*
- $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$*.*

Ako postoji jedinični element (jedinica) takav da važi $1 \cdot a = a = a \cdot 1$ za svako $a \in R$, onda kažemo da je R **prsten s jedinicom**. Prsten R je **komutativan prsten** ako važi $a \cdot b = b \cdot a$ za svako a i b iz R. Elemenat 0 zovemo nula prstena R.
Neki primeri prstena su skup realnih, racionalnih, kompleksnih i celih brojeva. Još jedan interesantan primer je skup celih brojeva po modulu n u oznaci $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = (Z_n, +_n, \cdot_n)$, gde su operacije $+_n$ i $\cdot_n$ sabiranje i množenje po modulu n. Ovo je komutativan prsten s jedinicom.

Definicija 3.3.2 (Polje)**.** *Polje* $(F, +, \cdot)$ *je komutativan prsten sa jedinicom takav da važi* $0 \neq 1$ *i svi elementi iz* $F \backslash \{0\}$ *imaju inverzni elemenat u odnosu na množenje.*

Na primer $(Z_n, +_n, \cdot_n)$ je polje ako i samo ako je n prost broj.
Prsten polinoma u oznaci $R[x]$ je prsten koji se sastoji od svih polinoma promenljive x s koeficijentima iz R. Dakle, svaki elemenat ovog prstena je oblika

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0, \tag{3.5}$$

gde su koeficijenti $a_n, a_{n-1}, ..., a_0$ iz R, a $n \in \mathbb{N}_0$.

Neka je $p(x) = a_m x^m + a_{m-1}x^{m-1} + ... + a_1 x + a_0$ polinom stepena m i $q(x) = b_r x^r + b_{r-1}x^{r-1} + ... + b_1 x + b_0$ polinom stepena r, koji pripadaju prstenu polinoma $R[x]$. Operacije sabiranja i množenja date su na sledeći način:

$$p(x)\cdot q(x) = \sum_{k=0}^{m+r} \left(\sum_{i+j=k} a_i b_j \right) x^k; \tag{3.6}$$

$$p(x) + q(x) = \sum_{k=0}^{\max\{m,r\}} (a_k + b_k)x^k, \text{ gde je } a_k = 0 \text{ za } k > m \text{ i } b_k = 0 \text{ za } k > r. \tag{3.7}$$

Definicija 3.3.3 (Ideal)**.** *Neprazan podskup I prstena R naziva se ideal ako važi:*

- $(\forall a, b \in I)\ \ a - b \in I$,
- $(\forall a \in I)(\forall r \in R)\ \ ar \in I$ *i* $ra \in I$.

Ako je dat ideal I prstena R može se definišati relacija $\sim$ na R sa

$$a \sim b \text{ ako i samo ako } a - b \in I.$$

Relacija $\sim$ je relacija kongruencije, te ako je $a \sim b$ kažemo da su a i b konguentni po modulu I. Klasa ekvivalencije elementa a iz R data je sa

$$\overline{a} = \{b | a - b \in I\} = \{a + r | r \in I\} = a + I. \tag{3.8}$$

Za bilo koji podskup $S \subset R$, minimalni ideal koji sadrži S označava se sa $\langle S \rangle$. Ako se S sastoji samo od jednog elementa a, onda je $\langle a \rangle = \{ra | r \in R\}$.

Definicija 3.3.4 (Kvocijentni prsten)**.** *Skup svih klasa ekvivalencija $\overline{a}$ naziva se kvocijentni prsten i označava se sa*

$$R/I = (\{a + I | a \in \mathbb{R}\}, +, \cdot), \tag{3.9}$$

gde su operacije sabiranja i množenja date sa

$$a + I + b + I = (a + b) + I \ \ i \ \ (a + I)(b + I) = (a\cdot b) + I.$$

Kvocijentni prsten naziva se još i faktor prsten.[7].

Sada se može definisati prsten koji je za ovo poglavlje najvažniji, a to je konvolucijski prsten polinoma.

Definicija 3.3.5 (Konvolucijski prsten polinoma)**.** *Neka je dat broj n. Konvolucijski prsten polinoma (ranga n) je kvocijentni prsten*

$$\mathcal{R} = \mathbb{Z}[x]/\langle x^n - 1 \rangle. \tag{3.10}$$

Važe jednakosti:

$$\begin{aligned} R_{(x^n-1)}[x^n] &= 1, \\ R_{(x^n-1)}[x^{n+1}] &= x, \\ &\vdots \\ R_{(x^n-1)}[x^{n+k}] &= x^{R_n[k]}, \end{aligned}$$

za bilo koji prirodan broj k.

[7]Primetimo analogiju sa definicijom faktor grupe $G/H = (\{aH | a \in G\}, \cdot)$, gde je G grupa s operacijom $\cdot$, H njena normalna podgrupa, a $aH\cdot bH \overset{\text{def}}{=} (a\cdot b)H$ (videti [19]).

Dakle elementi ovog prstena su polinomi stepena manjeg od n, s koeficijentima iz $\mathbb{Z}$.
Operacija sabiranja se definiše standardno, dok je operacija množenja data narednom formulom.
Neka je dat broj n, kao i polinomi $p(x) = a_k x^k + a_{k-1}x^{k-1} + ... + a_1 x + a_0$ i $q(x) = b_r x^r + b_{r-1}x^{r-1} + ... + b_1 x + b_0 \in \mathcal{R}$. Proizvod polinoma je dat sa

$$p(x) * q(x) = c_m x^m + c_{m-1}x^{m-1} + ... + c_1 x + c_0, \tag{3.11}$$

gde je $m = \max\{k, r\}$, a proizvoljan koeficijent $c_i = a_m b_{i+1} + a_{m-1}b_{i+2} + ... + a_{i+1}b_m + a_i b_0 + ... + a_1 b_{i-1} + a_0 b_i$.

Slično se definiše konvolucijski prsten polinoma po modulu m.

Definicija 3.3.6. *Konvolucijski prsten polinoma po modulu m je prsten polinoma stepena manjeg od n s koeficijentima iz skupa $\mathbb{Z}/m\mathbb{Z}$ i označava se sa*

$$\mathcal{R}_m = (\mathbb{Z}/m\mathbb{Z})[x]/\langle x^n - 1\rangle. \tag{3.12}$$

Operacije sabiranja i množenja definišu se isto, s tim što se još vrednost svakog koeficijenta c_i redukuje po modulu m.

Primer 3.3.1. Neka je $n = 3$. Izračunajmo konvolucijski proizvod polinoma $p(x) = a_2x^2+a_1x+a_0 = x^2 + 1$ i $q(x) = b_1x + b_0 = 2x + 7$ u $\mathcal{R}$ i $\mathcal{R}_4$.
$p(x) * q(x) = c_2x^2 + c_1x + c_0$, gde je
$c_2 = a_2b_0 + a_1b_1 = 7 + 0 = 7$
$c_1 = a_1b_0 + a_0b_1 = 0 + 2 = 2$
$c_0 = a_2b_1 + a_0b_0 = 2 + 7 = 9$
Dakle, $(x^2 + 1) * (2x + 7) = 7x^2 + 2x + 9$ u $\mathbb{Z}[x]/\langle x^3 - 1\rangle$.
Nakon redukovanja koeficijenata po modulu 4, dobijamo proizvod polinoma u $(\mathbb{Z}/4\mathbb{Z})[x]/\langle x^3 - 1\rangle$, a to je $3x^2 + 2x + 1$.

Dati polinomi mogu se pomnožiti na još jedan način. Prvo se pomnože na klasičan način, a zatim se dobijeni polinom redukuje tako da pripada $\mathbb{Z}[x]/\langle x^3 - 1\rangle$, odnosno po modulu $x^3 - 1$. Koristeći jednakosti iz definicije 3.3.5 dobijamo

$$\begin{aligned} p(x) * q(x) &= 2x^3 + 7x^2 + 2x + 7 \\ &= 2 + 7x^2 + 2x + 7 \\ &= 7x^2 + 2x + 9 \ \ u \ \ \mathbb{Z}[x]/\langle x^3 - 1\rangle. \end{aligned}$$

Naredna teorema upravo govori o tome.

Teorema 3.3.1. *Konvolucijski proizvod dva polinoma $p(x)$ i $q(x)$ iz $\mathcal{R} = \mathbb{Z}[x]/\langle x^n-1\rangle$ dat je sledećom formulom*

$$p(x) * q(x) = c(x), \ \ \textit{gde je} \ \ c_k = \sum_{i+j=R_n[k]} a_i b_j, \tag{3.13}$$

gde su a_i i b_j koeficijenti polinoma $p(x)$ i $q(x)$ respektivno.

Definicija 3.3.7. *Inverzni elemenat polinoma p po modulu m iz prstena polinoma je polinom q takav da važi*

$$R_m[pq] = 1. \tag{3.14}$$

Sada kada su definisani svi neophodni pojmovi, možemo se vratiti na NTRU kriptosistem. Biće predstavljena dva načina generisanja ključeva, postupka šifrovanja i dešifrovanja u NTRU kriptosistemu. Prvi postupak je preko cikličnih matrica, a drugi direktno preko polinoma.

Prvi način [15], [3]
NTRU kriptosistem se, kao što je prethodno spomenuto, opisuje kao kriptosistem (konvolucijskog) prstena polinoma. Međutim, relacija između javnoj i tajnog ključa definiše određenu rešetku, koja se zove NTRU rešetka. Baza rešetke može se dobiti iz javnog ključa, dok tajni ključ odgovara određenim kratkim vektorima ove rešetke. Stoga je prirodno da se napadi zasnivaju na pokušajima da se reši SVP problem u rešetki. Ipak, nije neophodno uvoditi rešetke u postupku šifrovanja i dešifrovanja.

Parametri kriptosistema
Najpre se fiksira prost broj n koji određuje konvolucijski prsten polinoma $\mathcal{R} = \mathbb{Z}[x]/\langle x^n - 1\rangle$. Dalje se definišu:
$\mathcal{D}_f$ - prostor dela tajnog ključa,
$\mathcal{D}_g$ - prostor dela tajnog ključa i
$\mathcal{D}_r$ - prostor polinoma za sakrivanje.

Ovi prostori su određeni celobrojnim parametrima d_f, d_g, d_r i sastoje se od "malih" polinoma, odnosno polinoma s koeficijentima iz skupa $\{0, 1\}$ ili $\{-1, 0, 1\}$. Konkretno, dati parametri određuju koliko će koeficijenata u polinomima biti jednako sa -1 ili 1 (ostali koeficijenti su 0) što se može videti u tabeli 4.

Prostor polinoma	**Broj koeficijenata jednakih sa** -1 **(za ternarne polinome)**	**Broj koeficijenata jednakih sa** 1
$\mathcal{D}_f$	$d_f - 1$	d_f
$\mathcal{D}_g$	d_g	d_g
$\mathcal{D}_r$	d_r	d_r

Tabela 4: Definisanje prostora malih (binarnih i ternarnih) polinoma.

Naredni pojam koji se uvodi je pojam ciklične matrice. Neka je dat vektor $x \in \mathbb{R}^n$. Njegova ciklična matrica je

$$[C^*x] = [x, Cx, ..., C^{n-1}x] = \begin{bmatrix} x_1 & x_n & x_{n-1} & \cdots & x_2 \\ x_2 & x_1 & x_n & \cdots & x_3 \\ x_3 & x_2 & x_1 & \cdots & x_4 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & x_{n-1} & x_{n-2} & \cdots & x_1 \end{bmatrix} \tag{3.15}$$

Koeficijenti polinoma f i g mogu se zapisati u obliku vektora $\vec{f}$ i $\vec{g}$. Tada je konvolucijski proizvod polinoma $f * g$ u stvari $[C^*\vec{f}]\vec{g}$.
U tabeli 5 predstavljeni su parametri kriptosistema, od kojih će $\vec{h}$ i H biti naknadno definisani.

Parametar	Opis	Javnost/Tajnost
n	stepen, prost broj	javan
q	veliki modul, ceo broj	javan
p	mali modul, polinom ili ceo broj	javan
d_f	ograničenje za f, ceo broj	javan
d_g	ograničenje za g, ceo broj	javan
d_r	ograničenje za r, ceo broj	javan
$\vec{f}$	vektor koeficijenata od f	tajan
$\vec{g}$	vektor koeficijenata od g	tajan
$\vec{h}$	vektor koeficijenata od h	javan
H	ciklična matrica $n \times n$	javna

Tabela 5: Parametri NTRU kriptosistema.

Napomena 5. *Pored toga što n mora biti prost broj, p i q moraju biti uzajamno prosti.*

Generisanje ključeva

Tajni ključ

Prvo se vrši odabir polinoma $f \in \mathcal{D}_f$ i $g \in \mathcal{D}_g$. Tajni ključ je kratak vektor $(\vec{f}, \vec{g})$ u $\mathbb{Z}^{2n}$. Dodatno, matrica $[C^*\vec{f}]$ mora biti invertibilna po modulu p i modulu q. Odgovarajuće inverzne matrice označavaju se sa $[C^*\vec{f}]_p^{-1}$ i $[C^*\vec{f}]_q^{-1}$.

Javni ključ $\vec{h}$ dobija se od tajnog ključa na sledeći način

$$[C^*\vec{f}]\vec{h} = R_q[p\vec{g}]. \tag{3.16}$$

Kako je $[C^*\vec{f}]$ invertibilna po modulu q, onda se $\vec{h}$ računa kao $\vec{h} = R_q\big[p[C^*\vec{f}]^{-1}\vec{g}\big]$.

Poslednji parametar koji nije definisan je ciklična matrica

$$H = [C^*\vec{h}]. \tag{3.17}$$

Rešetka je definisana svim celobrojnim vektorima $(v, w) \in \mathbb{Z}^{2n}$ koji zadovoljavaju jednačinu

$$w = R_q[Hv]. \tag{3.18}$$

Teorema 3.3.2. *Za svaki vektor (v, w) u rešetki važi da su i sve njegove ciklične rotacije $(C^k v, C^k w)$ takođe u rešetki, za $0 \leq k \leq n-1$.*

Neka je $\vec{h} = [h_0, h_1, ..., h_{n-1}]$ javni ključ. NTRU rešetka je $2n$-dimenzionalna rešetka generisana vektorima kolona matrice

$$L(B) = \left[\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ \hline h_0 & h_{n-1} & \cdots & h_1 & q & 0 & \cdots & 0 \\ h_1 & h_0 & \cdots & h_2 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{n-1} & h_{n-2} & \cdots & h_0 & 0 & 0 & \cdots & q \end{array}\right].$$

U pitanju je, dakle, blok matrica

$$L(B) = \left[\begin{array}{c|c} E & O \\ \hline H & qE \end{array}\right],$$

gde je E jedinična matrica, O nula matrica, qE matrica koja na glavnoj dijagonali ima samo brojeve q, a H matrica definisana u 3.17. Sve matrice su dimenzije $n \times n$.

Enkripcija
Postupak počinje tako što se najpre otvoreni tekst transformiše u vektor $m \in \mathbb{Z}^n$, s koeficijentima iz skupa $[-\frac{p}{2}, \frac{p}{2}]$ za parno p ili $[-\frac{p-1}{2}, \frac{p-1}{2}]$ za neparno p. Standard je da se uzima da je $p = 3$, te je ovo u stvari skup $\{-1, 0, 1\}$. Zatim se slučajno bira polinom sakrivanja r koji ima d_r koeficijenata jednakih sa 1, isto toliko koeficijenata jednakih sa -1, a ostalo su nule. Šifrat se zatim računa kao

$$c = R_q\big[[C^*\vec{h}]\vec{r} + m\big]. \tag{3.19}$$

Dekripcija
Da bi se dešifrovao šifrat c, prvo se računa a koje zadovoljava

$$a = R_q\big[[C^*\vec{f}]c\big], \tag{3.20}$$

tako da su sve koordinate od a u intervalu $[-q/2, q/2]$. Vektor m nalazi se kao

$$m = R_p\big[[C^*\vec{f}]_p^{-1}a\big], \tag{3.21}$$

tako da su koordinate u skupu $\{-1, 0, 1\}$.

Drugi način [20], [21]
Postavljanje parametara vrlo je slično, s tim što su vektor $\vec{h}$ i matrica H sada višak. Uslovi koji ti parametri moraju da zadovoljavaju su isti. Takođe se dodatno definiše prostor $\mathcal{D}_m$.

$\mathcal{D}_m$ - prostor polinoma otvorenog teksta m odnosno svih njegovih ispravnih reprezentacija.

Za svaki polinom iz $\mathcal{D}_m$ važi ograničenje da je broj koeficijenata jednakih sa 1 veći ili jednak od d_m, gde je d_m ceo broj, koeficijenata jednakih sa -1 takođe mora biti $\geq d_m$, a ostalo su nule.

Generisanje ključeva
Prvo se vrši odabir polinoma $f \in \mathcal{D}_f$ i $g \in \mathcal{D}_g$, a zatim se računaju inverzni polinomi polinoma f po modulima p i q, respektivno. Označimo ih sa f_p i f_q. Oni dakle moraju da zadovoljavaju

$$R_p[f * f_p] = 1 \quad \text{i} \tag{3.22}$$

$$R_q[f * f_q] = 1. \tag{3.23}$$

U slučaju da takvi ne postoje, ponovo se vrši odabir polinoma f, sve dok se postojeći inverzi ne nađu.

Javni ključ se računa na sledeći način

$$h = R_q[pf_q * g]. \tag{3.24}$$

Tajni ključ je par polinoma (f, f_p). Polinom g je takođe tajan.

Enkripcija
Otvoreni tekst koji se šalje prvo se pretvara u polinomni oblik $m \in \mathcal{D}_m$. Zatim se nasumično bira polinom sakrivanja $r \in \mathcal{D}_r$. Šifrovani tekst se dobija kao

$$c = R_q[r * h + m]. \tag{3.25}$$

Dekripcija
Da bi se dešifrovao šifrat c, najpre se računa

$$a = R_q[f * c], \tag{3.26}$$

gde kao i u prethodnom slučaju koeficijenti od a moraju biti iz intervala $[-q/2, q/2]$. Zatim se polinom a redukuje po modulu p

$$b = R_p[a]. \tag{3.27}$$

Polinom m se sada računa preko jednačine

$$m = R_p[f_p * b]. \tag{3.28}$$

Zašto ovo funkcioniše?
Kada se poruka m šifruje, prvo se generiše polinom sakrivanja r koji je primaocu nepoznat. Međutim, primalac računa

$$\begin{aligned} a &= R_q[f * c] \\ &= R_q[f * (r * h + m)] \\ &= R_q[f * (r * pf_q * g + m)] \\ &= R_q[pr * g + f * m] \ \ (\text{iz } R_q[f * f_q] = 1). \end{aligned}$$

Kako su koeficijenti polinoma m, r, f i g mali, sledi da su i koeficijenti konvolucijskih prizvoda $r * g$ i $f * m$ takođe mali, u odnosu na q. Kao rezultat toga, koeficijenti polinoma $pr * g + f * m$ su već u intervalu $[-q/2, q/2]$, ako su parametri dobro izabrani. Redukcija po modulu q u tom slučaju nema uticaja, odnosno $a = pr * g + f * m$, pa kada se a redukuje po modulu p, u stvari se redukuje ovaj polinom. Odatle se dobija polinom $b = R_p[f * m]$. Sada je još preostalo da se pomnože f_p i b, odnosno $f_p * b = f_p * f * m$, što daje ostatak m pri deljenju sa p.

Napomena 6. *Ako parametri nisu dobro odabrani, moguće je da se desi da koeficijenti polinoma $f * c = pr * g + f * m$ ne leže u intervalu $[-q/2, q/2]$, što bi dovelo do pogrešnog dešifrovanja. Ovo je bila motivacija za uvođenje šeme enkripcije NAEP (NTRU Assymetric Encryption Padding [22],[23]) a pogrešno dešifrovanje se koristilo i u jednom napadu na ovaj kriptosistem, opisan u [24].*

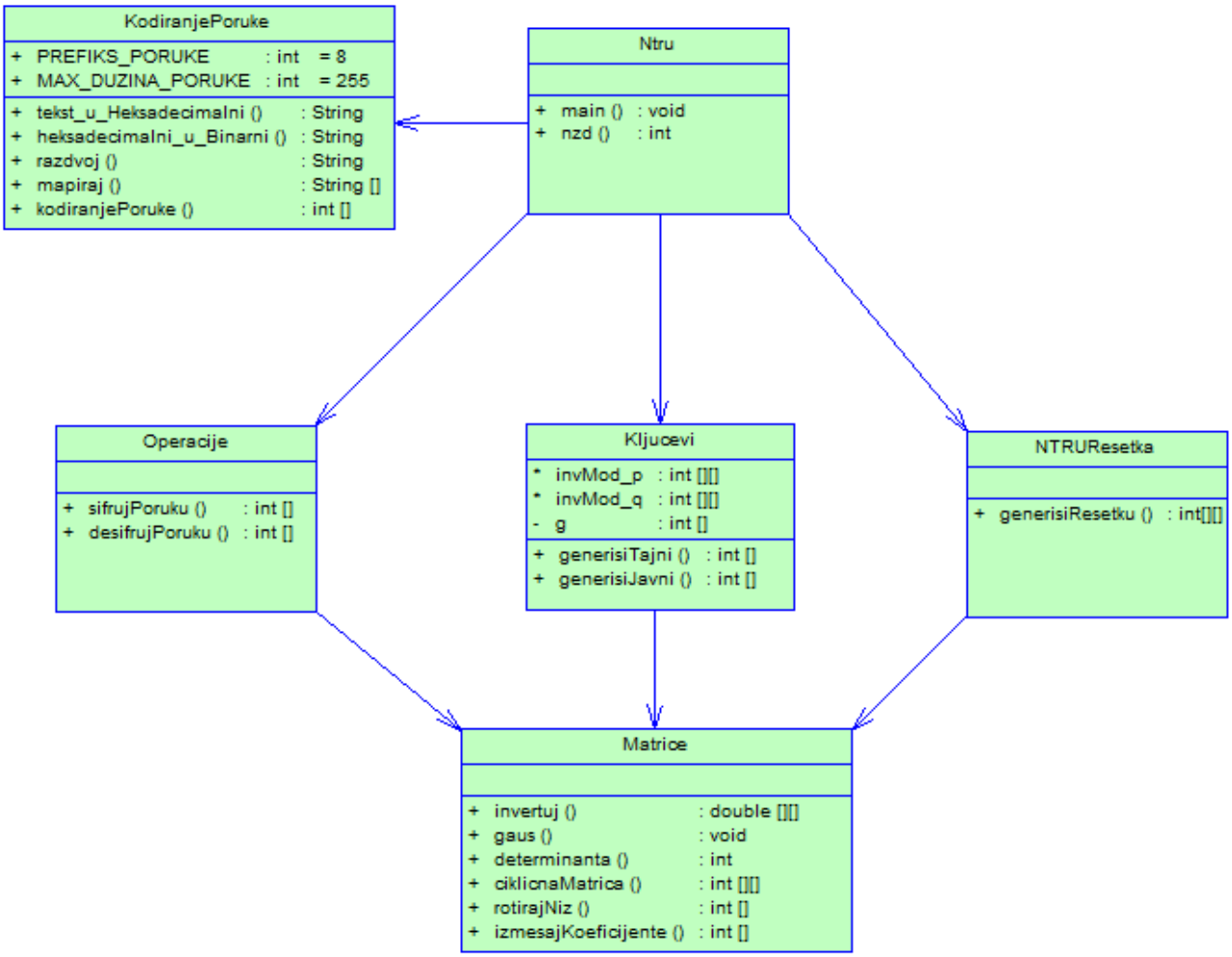
Praktičnost kriptosistema
Ako se posmatra prvi način generisanja ključeva, javni ključ je vektor dužine n sa elementima iz skupa $\{0, 1, ..., q-1\}$. Stoga on zahteva $O(n \log_2 q)$ bita u prostoru. Za drugi način opisivanja ovog kriptosistema osnovni podaci dati su u tabeli 6.

Objekat	**Veličina u bitovima**
Javni ključ	$n \log_2 q$
Tajni ključ	$2n \log_2 p$
Operacija	**Vreme**
Šifrovanje	$O(n^2)$
Dešifrovanje	$O(n^2)$

Tabela 6: Veličina javnog ključa i vreme operacija u NTRU kriptosistemu.

3.3.2 Implementacija NTRU kriptosistema

Implementacija NTRU kriptosistema realizovana je u programskom jeziku JAVA. Za razvojno okruženje korišćen je Eclipse. Na slici 9 prikazan je dijagram klasa.



Slika 9: NTRU dijagram klasa.

Da bi se operacija šifrovanja mogla primeniti na otvoreni tekst, tekstualna poruka mora se pretvoriti u polinomni oblik, tačnije u ternarni oblik. Dakle, ona se mora kodirati. Klasa KodiranjePoruke sadrži atribute MAX_DUZINA_PORUKE (255) što predstavlja najveći broj bajtova poruke koje možemo da šifrujemo i PREFIKS_PORUKE, koji predstavlja unapred određenu (8) dužinu dužine poruke u binarnom zapisu. Poruka koju želimo da šifrujemo prvo se metodom tekst_u_Heksadecimalni() pretvori u heksadecimalni zapis, a zatim metodom heksadecimalni_u_Binarni() u string format binarnog

zapisa. Dužina originalne poruke koja je zapisana u bitovima dodaje se ispred dobijenog stringa, a na kraju se dodaje dopuna (engl. *padding*) koja se sastoji od nula. Dužina "prve" dopune u bajtovima dobija se kada se od MAX_DUZINA_PORUKE oduzme stvarna dužina poruke, a zatim se dobijen broj pomnoži sa 8 kako bi se dobila dužina u bitovima. Neka je binarni zapis tekstualne poruke mbin. Dakle, poruka će pre konverzije iz binarnog u ternarni zapis imati oblik dužina||mbin||dopuna. Na primer, ako šifrujemo "AB", poruka će biti oblika 00000010||01000001 01000010||000...0, gde se 0 ponavlja $255 \cdot 8 - 16 = 2024$ puta. Metodom razdvoj() dobijeni string razdvaja se na stringove od po tri karaktera. Ako dužina stringa nije deljiva sa 3, dodaju se nule tako da bude deljiva. Zatim se metodom mapiraj() vrši mapiranje:

$$\{0,0,0\} \to \{0,0\}$$
$$\{0,0,1\} \to \{0,1\}$$
$$\{0,1,0\} \to \{0,-1\}$$
$$\{0,1,1\} \to \{1,0\}$$
$$\{1,0,0\} \to \{1,1\}$$
$$\{1,0,1\} \to \{1,-1\}$$
$$\{1,1,0\} \to \{-1,0\}$$
$$\{1,1,1\} \to \{-1,1\}.$$

Za prethodni primer dobili bismo niz 00001111001-1000-1000...0. Ukupno raspoloživ broj bitova za poruku u ternarnom zapisu dobija se preko formule (PREFIKS_PORUKE + MAX_DUZINA_PORUKE$\cdot 8 + 1)/3 \cdot 2 = 1366$. Ako ovaj broj nije deljiv parametrom n, dodaju se nule na kraj toliko da bude, kako bi se poruka mogla izdeliti na blokove dužine n. Na svaki zasebni blok primenjuje se postupak šifrovanja. Sve ove metode pozivaju se u metodi kodiranjePoruke() koja nam vraća niz s elementima iz skupa $\{-1, 0, 1\}$, koji predstavljaju koeficijente polinoma. Na primer, niz [1 1 0 -1 1] predstavlja polinom $1 + x - x^3 + x^4$.
Kodiranje poruke donekle je ispoštovalo standard IEEE P1363.1, koji se može pogledati na stranici `http://grouper.ieee.org/groups/1363/lattPK/`. U ovom dokumentu, pored navedenog, predlaže se da se ispred oblika dužina||mbin||dopuna doda još slučajno generisan niz bitova unapred određene dužine (db), što je ovde izostavljeno iz praktičnih razloga. U zavisnosti od toga koliku sigurnost želimo da postignemo, biramo parametar db. Na primer ako želimo 128-bitnu sigurnost izabraćemo db = 128, ako želimo 256-bitnu sigurnost izabraćemo da je db=256 i tako dalje. Takođe, s obzirom na to da se za parametar n uzimaju velike vrednosti (neke od preporučenih su 1087, 1171, 1499) formula za računanje maksimalne dužine poruke (N$\cdot 3/2/8$ - dužina$/8$ - db$/8$) nije primenjena, kako u radu nije rađeno direktno s polinomima, već matricama dimenzija $n \times n$, te primeri koji će naknadno biti predstavljeni ne bi bili pregledni. Stoga je za MAX_DUZINA_PORUKE uzeta fiksna vrednost.

U klasi Kljucevi generišu se tajni ključ (f, g) i javni ključ h. Atributi ove klase su InvMod_p, invMod_q, što su u stvari inverzne matrice ciklične matrice od f, po modulima p i q respektivno i drugi deo tajnog ključa, g. U nastavku je prikazan kod ove klase.

```
import java.math.BigInteger;

public class Kljucevi {

        int[][] InvMod_q;
        int[][] InvMod_p;
        private int[] g;
```

```
public int[] generisiTajni(int n, int p, int q, int df, int dg){
      int det = 0;
      int[] f = new int[n];
      g = new int[n];
      int indeks = 0;
      for(int i=0;i<dg;i++){
            g[indeks]=1;
            indeks++;
            g[indeks]=-1;
            indeks++;
      }
      g = Matrice.izmesajKoeficijente(g);
      indeks = 0;
      for(int i=0;i<df;i++){
        f[indeks]=1;
        indeks++;
        if(i<df-1){
            f[indeks]=-1;
            indeks++;
        }
      }
  while(det == 0){
     f = Matrice.izmesajKoeficijente(f);
     double[][] R = new double[n][n];
     int[][] C_f = Matrice.ciklicnaMatrica(f);
     for(int i=0;i<n;i++){
        for(int j=0;j<n;j++){
           R[i][j]=(double)C_f[i][j];
        }
     }
     det = Matrice.determinanta(C_f,n);
     if(det!=0){
         int k=1;
         if(det<0){
            k=-1;
         }
      double[][] I = Matrice.invertuj(R);
      int[][] Adj1 = new int[n][n];
      for(int i=0;i<n;i++){
          for(int j=0;j<n;j++){
                Adj1[i][j]=Math.round((float)I[i][j]*det*k);
          }
      }
      det=Math.abs(det);
      int inverzni_q =
      BigInteger.valueOf(det).modInverse(
      BigInteger.valueOf(q)).intValue();
      InvMod_q = new int[n][n];
```

```
        for(int i=0;i<n;i++){
                for(int j=0;j<n;j++){
                        InvMod_q[i][j] = inverzni_q*Adj1[i][j] % q;
                        if(InvMod_q[i][j] <0){
                            InvMod_q[i][j] = InvMod_q[i][j] + q;
                        }
                }
        }
        int inverzni_p =
        BigInteger.valueOf(det).modInverse(
        BigInteger.valueOf(p)).intValue();
        InvMod_p = new int[n][n];
        for(int i=0;i<n;i++){
            for(int j=0;j<n;j++){
               InvMod_p[i][j] = inverzni_p*Adj1[i][j] % p;
               if(InvMod_p[i][j] <0){
                  InvMod_p[i][j] = InvMod_p[i][j] + p;
               }
            }
        }
       }
       else{
         System.out.println("Matrica nije invertibilna!");
       }
    }
        int[] tajni = new int[2*n];
        for(int i=0;i<n;i++){
          tajni[i] = f[i];
        }
        for(int i=n;i<2*n;i++){
          tajni[i] = g[i-n];
        }
        System.out.println("Tajni kljuc je");
        for(int i=0;i<2*n;i++){
                System.out.print(tajni[i]+" ");
        }
 return f;
}

  public int[] generisiJavni(int n, int p, int q){

        int[] h = new int[n];
        for(int i=0;i<n;i++){
                for(int j=0;j<n;j++){
                        h[i]+=p*InvMod_q[i][j]*g[j];
                }
        }
        System.out.println("Javni kljuc je");
        for(int i=0;i<n;i++){
```

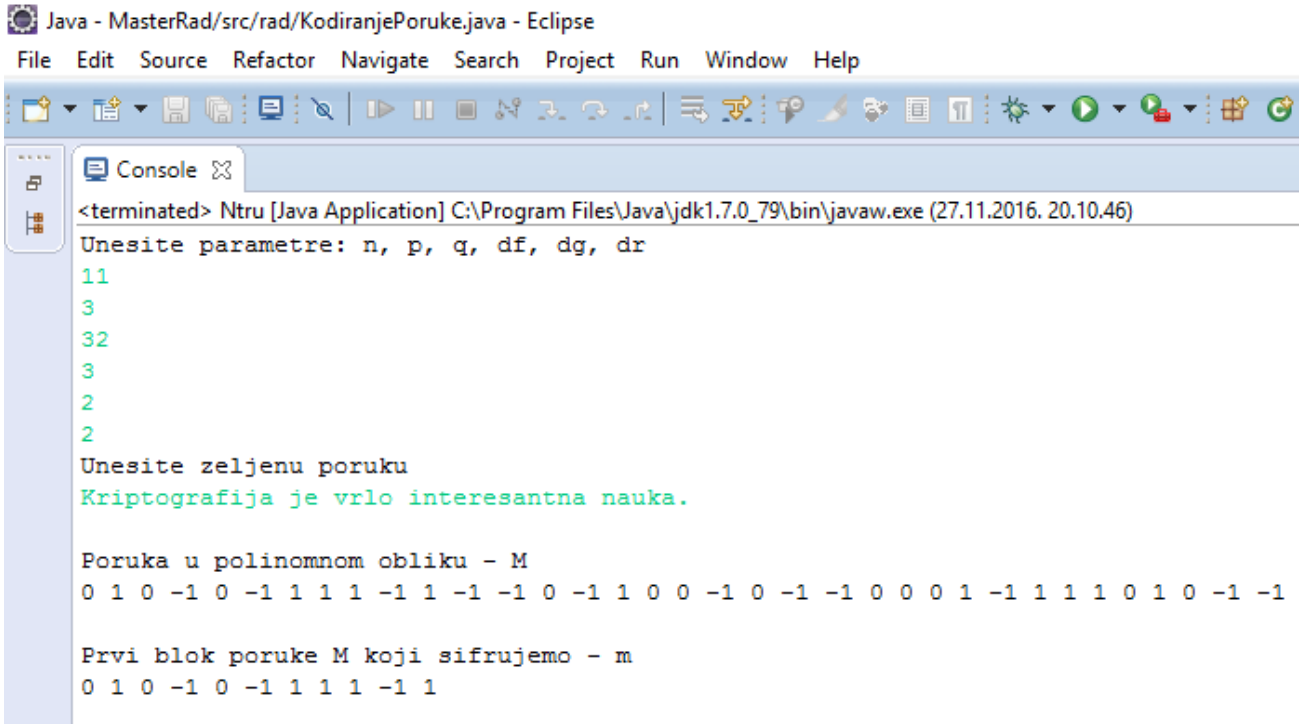
```
                h[i]=h[i] % q;
                if(h[i]<0){
                        h[i]=h[i]+q;
                }
                System.out.print(h[i]+" ");
        }
        return h;
    }

}
```

Naredni korak je šifrovanje poruke koje je omogućeno metodom sifrujPoruku(). Neka je M poruka u ternarnom obliku. Ova metoda prima parametre: n, blok dužine n poruke M, zatim javni ključ h, modul q i broj dr. Operacije sa matricama i nizovima definisane su u klasi Matrice [8]. Metodom desifrujPoruku() poruka M se dešifruje. U klasi NTRUresetka se nalazi metoda generisiResetku() kojom se generiše odgovarajuća NTRU rešetka, dok se u klasi Ntru nalazi se main() metoda i tu se pozivaju glavne metode.

U naredna dva primera predstavljen je deo rada u JAVA programskom jeziku.

Primer 3.3.2. Neka je sigurnosni parametar n = 11, a poruka koju želimo da šifrujemo "Kriptografija je vrlo interesantna nauka." Njen ternarni oblik je M = [0 1 0 -1 0 -1 1 1 1 -1 1 -1 -1 0 -1 1 0 0 -1 0 -1 -1 0 0 0 1 -1 1 1 1 0 1 0 -1 -1 1 0 1 -1 -1 0 -1 1 0 0 0 0 -1 -1 1 0 0 1 1 -1 0 1 1 0 0 -1 1 1 -1 0 0 1 1 1 1 0 0 1 0 0 -1 1 1 -1 0 -1 1 1 1 1 0 0 1 0 1 -1 1 1 -1 0 1 0 1 1 -1 1 1 1 0 1 0 -1 0 -1 0 0 0 1 1 -1 0 1 1 0 1 0 1 1 -1 0 -1 0 1 1 1 1 -1 1 0 1 1 1 1 -1 0 -1 1 -1 -1 1 0 1 0 0 0 0 -1 -1 -1 0 1 -1 1 1 1 0 1 0 1 1 -1 0 0 1 1 1 1 0 0 1 0 1 0 1 1 -1 0 0 1 -1 -1 1 -1 1 0 0 -1 -1 -1 0 0 1 1 1 -1 -1 0 ... 0].



Slika 10: Izbor parametara, poruka u ternarnom obliku (M) i prvi blok koji šifrujemo (m).

[8] Metoda invertovanja matrice Gausovom metodom eliminacije, tačnije invertuj() i gaus() preuzete su sa stranice `http://www.sanfoundry.com/java-program-find-inverse-matrix/`.

Ciklicna matrica C vektora f je

0	1	1	0	-1	1	0	-1	0	0	0
0	0	1	1	0	-1	1	0	-1	0	0
0	0	0	1	1	0	-1	1	0	-1	0
0	0	0	0	1	1	0	-1	1	0	-1
-1	0	0	0	0	1	1	0	-1	1	0
0	-1	0	0	0	0	1	1	0	-1	1
1	0	-1	0	0	0	0	1	1	0	-1
-1	1	0	-1	0	0	0	0	1	1	0
0	-1	1	0	-1	0	0	0	0	1	1
1	0	-1	1	0	-1	0	0	0	0	1
1	1	0	-1	1	0	-1	0	0	0	0

Slika 11: Ciklična matrica vektora f, tj. prvog dela tajnog ključa.

Inverzna matrica matrice C po modulu q je

28	1	7	12	7	13	20	8	5	14	14
14	28	1	7	12	7	13	20	8	5	14
14	14	28	1	7	12	7	13	20	8	5
5	14	14	28	1	7	12	7	13	20	8
8	5	14	14	28	1	7	12	7	13	20
20	8	5	14	14	28	1	7	12	7	13
13	20	8	5	14	14	28	1	7	12	7
7	13	20	8	5	14	14	28	1	7	12
12	7	13	20	8	5	14	14	28	1	7
7	12	7	13	20	8	5	14	14	28	1
1	7	12	7	13	20	8	5	14	14	28

Inverzna matrica matrice C po modulu p je

1	0	0	1	2	0	2	2	2	1	2
2	1	0	0	1	2	0	2	2	2	1
1	2	1	0	0	1	2	0	2	2	2
2	1	2	1	0	0	1	2	0	2	2
2	2	1	2	1	0	0	1	2	0	2
2	2	2	1	2	1	0	0	1	2	0
0	2	2	2	1	2	1	0	0	1	2
2	0	2	2	2	1	2	1	0	0	1
1	2	0	2	2	2	1	2	1	0	0
0	1	2	0	2	2	2	1	2	1	0
0	0	1	2	0	2	2	2	1	2	1

Slika 12: Inverzne matrice matrice C po modulima 32 i 3.

```
Tajni kljuc je
0 0 0 0 -1 0 1 -1 0 1 1 1 0 0 0 1 0 -1 0 0 -1 0

Prvi deo tajnog kljuca je
0 0 0 0 -1 0 1 -1 0 1 1

Javni kljuc je
3 24 18 18 16 14 25 5 15 14 8

Vektor sakrivanja je
1 0 -1 -1 0 0 0 0 0 1 0

Sifrat je
24 21 23 4 31 14 7 22 17 18 13

Vektor a je
5 3 0 -5 -2 3 -5 -4 2 4 1

Poruka m nakon desifrovanja je
0 1 0 -1 0 -1 1 1 1 -1 1
```

Slika 13: Tajni ključ, vektor f, vektor sakrivanja r, šifrat, vektor a i poruka m nakon dešifrovanja.

Dakle, dobili smo upravo onaj deo poruke koji smo šifrovali.

Primalac će postupak ponavljati za svaki blok od po 11 elemenata, sve dok ne dobije celu poruku M = [0 1 0 -1 0 -1 1 1 1 -1 1 -1 -1 0 -1 1 0 0 -1 0 -1 -1 0 0 0 1 -1 1 1 1 0 1 0 -1 -1 1 0 1 -1 -1 0 -1 1 0 0 0 0 -1 -1 1 0 0 1 1 -1 0 1 1 0 0 -1 1 1 -1 0 0 1 1 1 1 0 0 1 0 0 -1 1 1 -1 0 -1 1 1 1 1 0 0 1 0 1 -1 1 1 -1 0 1 0 1 1 -1 1 1 1 0 1 0 -1 0 -1 0 0 0 1 1 -1 0 1 1 0 1 0 1 1 -1 0 -1 0 1 1 1 1 -1 1 0 1 1 1 1 -1 0 -1 1 -1 -1 1 0 1 0 0 0 0 -1 -1 -1 0 1 -1 1 1 1 0 1 0 1 1 -1 0 0 1 1 1 1 0 0 1 0 1 0 1 1 -1 0 0 1 -1 -1 1 -1 1 0 0 -1 -1 -1 0 0 1 1 1 -1 -1 0 .... 0]. Zatim se odbiju nule koje su dodate kako bi ukupno raspoloživ broj bitova (1366) bio deljiv sa 11, a to je 9 nula. Dalje se vrši obrnuto mapiranje:

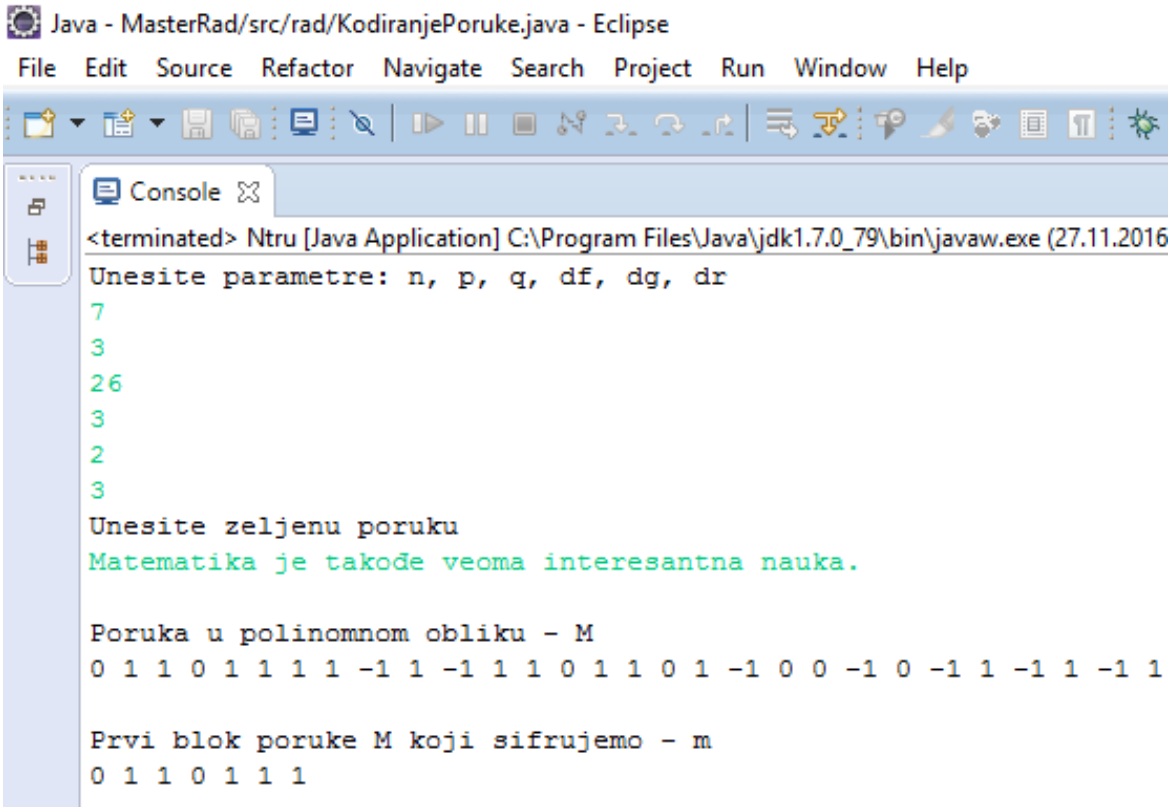
$$\begin{aligned}
\{0,0\} &\to \{0,0,0\} \\
\{0,1\} &\to \{0,0,1\} \\
\{0,-1\} &\to \{0,1,0\} \\
\{1,0\} &\to \{0,1,1\} \\
\{1,1\} &\to \{1,0,0\} \\
\{1,-1\} &\to \{1,0,1\} \\
\{-1,0\} &\to \{1,1,0\} \\
\{-1,1\} &\to \{1,1,1\} \\
\{-1,-1\} &\to \{1,1,1\}.
\end{aligned}$$

Nakon mapiranja dobija se oblik dužina||mbin||dopuna = [0 0 1 0 1 0 0 1 0 1 0 0 1 0 1 1 0 1 1 1 0 0 1 0 0 1 1 0 1 0 0 1 0 1 1 1 0 0 0 0 0 1 1 1 0 1 0 0 0 1 1 0 1 1 1 1 0 1 1 0 0 1 1 1 0 1 1 1 0 0 1 0 0 1 1 0

0 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 0 1 0 1 0 0 1 1 0 0 0 0 1 0 0 1 0 0 0 0 0 0 1 1 0 1 0 1 0 0
1 1 0 0 1 0 1 0 0 1 0 0 0 0 0 0 1 1 1 0 1 1 0 0 1 1 1 0 0 1 0 0 1 1 0 1 1 0 0 0 1 1 0 1 1 1 1 0 0 1 0 0 0
0 0 0 1 1 0 1 0 0 1 0 1 1 0 1 1 1 0 0 1 1 1 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 0 0 1 0 0 1 1 0 0 1 0 1 0 1 1
1 0 0 1 1 0 1 1 0 0 0 0 1 0 1 1 0 1 1 1 0 0 1 1 1 0 1 0 0 0 1 1 0 1 1 1 0 0 1 1 0 0 0 0 1 0 0 1 0 0 0 0 0
0 1 1 0 1 1 1 0 0 1 1 0 0 0 0 1 0 1 1 1 0 1 0 1 0 1 1 0 1 0 1 1 0 1 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 ... 0].
Prvih 8 bitova predstavljaju dužinu poruke, a to je upravo 41. Dužina poruke u bitovima je 328, te kad se od maksimalne dužine poruke u bitovima (2040) oduzme ovaj broj, dobija se 1712 i to je dužina prve dopune. Takođe, jedna nula je dodata pre konverzije iz binarnog u ternarni oblik, kako bi dužina stringa bila deljiva sa 3, te je dužina dopune 1713. Ono što ostaje je binarni zapis tekstualne poruke. U narednom koraku se binarni zapis konvertuje u heksadecimalni, a to je 4B 72 69 70 74 6F 67 72 61 66 69 6A 61 20 6A 65 20 76 72 6C 6F 20 69 6E 74 65 72 65 73 61 6E 74 6E 61 20 6E 61 75 6B 61 2E. Koristeći UTF-8 tabelu ovaj zapis se pretvara u tekstualni, a to je baš otvoreni tekst s početka.

U narednom primeru biće prikazana i NTRU rešetka.

Primer 3.3.3. Neka je sada parametar n = 7, a poruka koju želimo da šifrujemo ”Matematika je takođe veoma interesantna nauka.” Poruka u ternarnom obliku je [0 1 1 0 1 1 1 1 -1 1 -1 1 1 0 1 1 0 1 -1 0 0
-1 0 -1 1 -1 1 -1 1 -1 1 0 0 0 0 -1 -1 0 -1 0 1 1 -1 0 1 1 0 0 -1 -1 -1 0 0 1 1 1 1 0 0 1 0 0 -1 1 1 -1 0 -1 1
1 1 1 0 0 1 0 1 -1 0 0 -1 0 0 1 -1 1 -1 1 0 1 0 1 0 -1 1 1 0 -1 0 -1 0 -1 0 1 1 0 0 1 0 -1 0 -1 0 0 0 1 -1 -1
1 0 0 1 0 -1 -1 -1 1 -1 1 -1 1 -1 1 0 0 0 0 -1 0 -1 0 0 0 1 1 -1 0 1 1 0 1 0 1 1 -1 0 -1 0 1 1 1 1 -1 1 0 1 1
1 1 -1 0 -1 1 -1 -1 1 0 1 0 0 0 0 -1 -1 -1 0 1 -1 1 1 1 0 1 0 1 1 -1 0 0 1 1 1 1 0 0 1 0 1 0 1 1 -1 0 0 1 -1
-1 1 -1 1 0 0 -1 -1 -1 0 0 1 1 1 -1 -1 0 ... 0].



Slika 14: Poruka i izbor parametara sada su drugačiji.

```
Ciklicna matrica C vektora f je

0       -1      1       0       1       -1      1
1       0       -1      1       0       1       -1
-1      1       0       -1      1       0       1
1       -1      1       0       -1      1       0
0       1       -1      1       0       -1      1
1       0       1       -1      1       0       -1
-1      1       0       1       -1      1       0
```

Slika 15: Ciklična matrica vektora f.

```
Inverzna matrica matrice C po modulu q je

18      11      17      21      18      16      4
4       18      11      17      21      18      16
16      4       18      11      17      21      18
18      16      4       18      11      17      21
21      18      16      4       18      11      17
17      21      18      16      4       18      11
11      17      21      18      16      4       18
Inverzna matrica matrice C po modulu p je

0       2       0       1       2       0       2
2       0       2       0       1       2       0
0       2       0       2       0       1       2
2       0       2       0       2       0       1
1       2       0       2       0       2       0
0       1       2       0       2       0       2
2       0       1       2       0       2       0
```

Slika 16: Inverzne matrice matrice C po modulima 26 i 3.

```
Tajni kljuc je
0 1 -1 1 0 1 -1 0 0 0 1 -1 1 -1

Prvi deo tajnog kljuca je
0 1 -1 1 0 1 -1

Javni kljuc je
19 20 17 9 18 5 16

Vektor sakrivanja je
1 -1 0 1 -1 1 -1

Sifrat je
9 7 18 8 22 14 5

Vektor a je
-2 8 -9 12 -12 10 -2

Poruka m nakon desifrovanja je
0 1 1 0 1 1 1
```

Slika 17: Ostali podaci.

```
NTRU resetka je

1       0       0       0       0       0       0       0       0       0       0       0       0       0
0       1       0       0       0       0       0       0       0       0       0       0       0       0
0       0       1       0       0       0       0       0       0       0       0       0       0       0
0       0       0       1       0       0       0       0       0       0       0       0       0       0
0       0       0       0       1       0       0       0       0       0       0       0       0       0
0       0       0       0       0       1       0       0       0       0       0       0       0       0
0       0       0       0       0       0       1       0       0       0       0       0       0       0
19      16      5       18      9       17      20      26      0       0       0       0       0       0
20      19      16      5       18      9       17      0       26      0       0       0       0       0
17      20      19      16      5       18      9       0       0       26      0       0       0       0
9       17      20      19      16      5       18      0       0       0       26      0       0       0
18      9       17      20      19      16      5       0       0       0       0       26      0       0
5       18      9       17      20      19      16      0       0       0       0       0       26      0
16      5       18      9       17      20      19      0       0       0       0       0       0       26
```

Slika 18: NTRU rešetka.

4 Novija istraživanja i rezultati

Oded Regev[9] (Oded Regev) je 2004. godine u svom radu [25] uveo novi kriptosistem zanovan na Ajtai-Dvork kriptosistemu, gde je dao nekoliko poboljšanja rezultatima do kojih su došli Ajtai i Dvork u [26]. Glavna prednost bila je da razbijanje modifikovanog kriptosistema implicira rešavanje problema jedinstvenog najkraćeg vektora za faktor $\gamma = \tilde{O}(n^{3/2})$ dok je, podsetimo se, u originalnom radu faktor bio $\gamma \approx n^8$. S obzirom na to da uSVP$_\gamma$ problem može da postane samo teži kako faktor γ opada, sledi da je Regevov kriptosistem takođe siguran. Nakon toga, on je uveo **problem učenja s greškama** (engl. *learning with errors problem*). Na osnovu Regevovog rada [27], Kris Pajkert (Chris Peikert) je izumeo kriptosistem čija se sigurnost zasniva na jednoj varijanti problema SVP (GapSVPγ) umesto na problemu uSVP$_\gamma$ [28].

Definišimo još jedan problem koji je uveo Ajtai u svom čuvenom radu [4].

Definicija 4.0.1 (Mala celobrojna rešenja (SIS$_{n,q,\beta,m}$))**.** *Ako je dat modul q, matrica $A \in \mathbb{Z}_q^{n\times m}$, gde je $m \geq n$ i realni broj $\beta > 0$, naći ne-nula vektor $u \in \mathbb{Z}^m$ takav da je*

$$R_q[Au] = 0 \quad i \quad \|u\| \leq \beta.$$

Pretpostavlja se da je β odabrano tako da rešenja postoje. Takođe, vektori oblika $x = qe_i$, gde je $e_i = (0, 0, ..., 1, ..., 0)$ vektor koji ima sve nule i jedinicu na i-tom mestu, trivijalno zadovoljavaju jednačinu $R_q[Ax] = 0$, te se za β uglavnom uzima da je manje od q, kako bi se ovi vektori isključili iz rešenja. U terminima modularnih matrica, ovaj problem je jednak problemu traženja vektora dužine najviše β u rešetki $\Lambda_q^\perp(A)$. U svom radu [29] Daniele Mićanco i Oded Regev pokazali su da je rešavanje SVP problema u slučajno odabranoj rešetki $\Lambda_q^\perp(A)$ (matrica A bira se slučajno i uniformno iz $\mathbb{Z}_q^{n\times m}$) teško najmanje koliko rešavanje SIS problema, s obzirom na to da je β izabrano tako da najkraći vektori u rešetki zadovoljavaju svojstvo traženo u SIS problemu. Ajtai je dokazao narednu teoremu.

Teorema 4.0.1. *Za bilo koji polinom $m = p(n)$, $\beta > 0$ i dovoljno veliko $q \geq \beta \cdot p(n)$, rešavanje SIS$_{n,q,\beta,m}$ s nezanemarljivom verovatnoćom je teško najmanje koliko i rešavanje problema GapSVP$_\gamma$ i SIVP$_\gamma$ za proizvoljnu $n-$dimenzionalnu rešetku, odnosno u najtežem slučaju, za neko $\gamma = \beta \cdot p(n)$.*

Nakon ovog otkrića, usledili su još jači rezultati, kao na primer u radu Mićanca i Regeva iz 2004. godine [30] gde je faktor $\gamma = \tilde{O}(n)$, za dobar izbor parametra β, sa modulom $q \approx \beta \cdot \tilde{O}(n\sqrt{m})$. U radu [31], 2013. godine, Mićanco i Pajkert su poboljšali granicu za q na $\beta \cdot n^\varepsilon$, za bilo koju konstantu $\varepsilon > 0$.

4.1 Učenje s greškama

Kao što je prethodno spomenuto, Oded Regev je 2005. godine uveo problem učenja s greškama u kriptografiju. Pre formalne definicije ovog problema, potrebno je opisati LWE raspodelu.

Neka je $q \geq 2$ celobrojni modul, $s \in \mathbb{Z}_q^n$ "tajni" vektor i χ raspodela verovatnoće na $\mathbb{Z}_q$. Raspodela $A_{s,\chi}$ na skupu $\mathbb{Z}_q^n \times \mathbb{Z}_q$ definiše se na sledeći način.
$A_{s,\chi}$:

- birati vektor $a \in \mathbb{Z}_q^n$ slučajno i uniformno,
- birati grešku $e \in \mathbb{Z}_q$ raspodelom χ,
- vratiti $R_q[(a, \langle a, s\rangle + e)]$.

[9] Oded Regev je profesor racunarstva na Univerzitetu u Njujorku.

Definicija 4.1.1 (Problem učenja s greškama (LWE)). *Neka su dati parametri $n \geq 1$, $q \geq 2$, raspodela verovatnoće χ na $\mathbb{Z}_q$ i proizvoljan broj nezavisnih uzoraka iz raspodele $A_{s,\chi}$. Naći s.*

U terminima modularnih matrica, ovaj problem predstavlja problem dekodiranja ograničenog rastojanja u rešetki $\Lambda_q(A)$. Posmatrajmo m LWE uzoraka $(a_i, b_i = \langle a_i, s\rangle + e_i)$ raspodele $A_{s,\chi}$. Neka je matrica A formata $n \times m$ takva da su joj kolone vektori $a_i \in \mathbb{Z}_q^n$, $i = 1, 2, ..., m$. Vrste ove matrice generišu rešetku $\Lambda_q(A) = \{y \in \mathbb{Z}^m | y = R_q[A^T x],$ za neko $x \in \mathbb{Z}^n\}$. Tajni vektor s iz LWE problema sada odgovara vektoru rešetke $A^T s$. Elementi vektora $A^T s$ su skalarni proizvodi $\langle a_i, s\rangle$, za $i = 1, 2, ..., m$. Kako je $b = (b_1, b_2, ..., b_m)$ i $e = (e_1, e_2, ..., e_m)$ imamo u stvari

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} \langle a_1, s\rangle \\ \langle a_2, s\rangle \\ \vdots \\ \langle a_m, s\rangle \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix}. \tag{4.1}$$

Cilj LWE problema je naći vektor s što je ekvivalentno nalaženju vektora $A^T s$ u rešetki. Problem LWE može se zato posmatrati i kao problem nalaženja najbližeg vektora u rešetki za dati vektor mete $b = A^T s + e$. U zavisnosti od izbora vektora greške e, vektor $A^T s$ će biti najbliži vektor vektoru b rešetke $\Lambda_q(A)$. U praksi se najčešće zahteva da je vektor greške e izabran tako da je ograničen s velikom verovatnoćom, pa se na taj način dobija ekvivalencija s problemom dekodiranja ograničenog rastojanja (BDD).
LWE problem se često opisuje i kao "dualni" problem SIS problema, pošto su, podsetimo se, rešetke $\Lambda_q(A)$ i $\Lambda_q^{\perp}(A)$ međusobno dualne.

Još jedan problem učenja s greškama uveli su Pajkert, Regev i Vadim Ljubaševski (Vadim Lyubashevsky) u radu iz 2010. godine "On ideal lattices and learning with errors over rings" [32], a to je **problem učenja s greškama u prstenu** ili skraćeno Ring-LWE. Ring-LWE problem je parametrizovan prstenom R ranga n, nad skupom celih brojeva, celobrojnim modulom $q \geq 2$ koji definiše kvocijentni prsten R/qR i raspodelom greške χ nad R. Prvo se definiše Ring-LWE raspodela, tačnije familija raspodela.

Za "tajni" vektor $s \in R/qR$, raspodela $A_{s,\chi}$ na skupu $R/qR \times R/qR$ definiše se na sledeći način.

- birati $a \in R/qR$ slučajno i uniformno,
- birati grešku $e \in R$ raspodelom χ,
- vratiti $R_q[(a, a \cdot s + e)]$.

Definicija 4.1.2 (Problem učenja s greškama u prstenu (Ring-LWE)). *Neka su dati parametri $n \geq 1$, $q \geq 2$, raspodela verovatnoće χ na R i proizvoljan broj nezavisnih uzoraka iz raspodele $A_{s,\chi}$. Naći s.*

Ovaj problem može se smatrati kao specijalan slučaj LWE problema, gde jedan uzorak $(a, a \cdot s + e)$ sa slučajnim $a \in R/qR$ odgovara n LWE uzorcima $(a_i, \langle a_i, s\rangle + e)$ sa slučajnim $a_i \in \mathbb{Z}_q^n$.

4.1.1 Kriptosistem zasnovan na LWE problemu

Prva verzija kriptosistema, zajedno sa dokazom o sigurnosti opisana je u Regevovom radu [27]. Nakon toga je Kris Pajkert[10] doprineo značajnom poboljšanju efikasnosti ovog kriptosistema u svom radu [33]. Kriptosistem koji će ovde biti opisan je predstavljen u radu Regeva i Mićanca [3]. On je skoro identičan Pajkertovom kriptosistemu, sem što je uveden još jedan parametar (r).

[10] Kris Pajkert, rođen 1978. godine, profesor je računarstva i kriptografije na Univerzitetu u Mičigenu.

Najpre se definiše takozvani *odlučujući problem učenja s greškama* kao što je to učinjeno u [3]. Neka su dati celi brojevi m, $n \geq 1$, $q \geq 2$ i funkcija raspodele χ na skupu $\mathbb{Z}_q$ (najčešće se uzima normalna raspodela sa zaokruženim vrednostima (engl. *rounded normal distribution*)).
Ulaz je par (A, v), gde je matrica $A \in \mathbb{Z}_q^{m \times n}$ izabrana uniformno, a vektor v je ili izabran uniformno iz skupa $\mathbb{Z}_q^m$ ili je izabran kao $v = As + e$, gde je s izabran uniformno iz $\mathbb{Z}_q^n$, a $e \in \mathbb{Z}_q^m$ izabran raspodelom χ^m. Cilj je razlikovati ova dva slučaja sa nezanemarljivom verovatnoćom.

Za LWE problem se veruje da je veoma težak, za dobar izbor parametara, s obzirom na to da najbolji algoritam rešava ovaj problem u eksponencijalnom vremenu (videti [27]). Redukcija najtežeg slučaja problema GapSVP$_\gamma$ na LWE problem opisana je u [27], međutim u pitanju je "kvantna" redukcija, odnosno aloritam koji vrši redukciju je kvantni. Dakle, nalaženje efikasnog algoritma koji rešava problem učenja s greškama implicirao bi postojanje efikasnog kvantnog algoritma koji rešava GapSVP$_\gamma$ problem.
Regev je u svom radu dokazao narednu teoremu.
Neka je ψ_α raspodela na $\mathbb{Z}_q$ koja se dobija od normalne raspodele čija je srednja vrednost 0, a standardna devijacija $\frac{\alpha q}{\sqrt{2\pi}}$, gde je svaka vrednost zaokružena na najbliži ceo broj i redukovana po modulu q.

Teorema 4.1.1. *Za bilo koji polinom $m \leq p(n)$, prost modul $q \leq p(n)$ i raspodelu ψ_α, gde je $\alpha q > \sqrt{n}$, rešavanje LWE problema je teško najmanje koliko i kvantno rešavanje GapSVP$_\gamma$ i SIVP$_\gamma$ problema za proizvoljnu $n-$dimenzionalnu rešetku, gde je $\gamma = \tilde{O}(n/\alpha)$.*

Parametri

- celi brojevi n, m, l, t, r, q,
- realan broj $\alpha > 0$.

Prostor poruka je $\mathbb{Z}_t^l$. Definiše se funkcija $f : \mathbb{Z}_t^l \to \mathbb{Z}_q^l$, gde je

$$f(z_1, z_2, ..., z_l) = (\lfloor z_1 q/t \rceil, \lfloor z_2 q/t \rceil, ..., \lfloor z_l q/t \rceil),$$

a z_i su iz skupa $\mathbb{Z}_t$. Takođe se definiše i njena inverzna funkcija $f^{-1} : \mathbb{Z}_q^l \to \mathbb{Z}_t^l$

$$f(z'_1, z'_2, ..., z'_l) = (\lfloor z'_1 t/q \rceil, \lfloor z'_2 t/q \rceil, ..., \lfloor z'_l t/q \rceil),$$

gde su z'_i elementi skupa $\mathbb{Z}_q$.

Napomena 7. *Sa $\lfloor \cdot \rceil$ označena je funkcija zaokruživanja broja na najbliži ceo broj.*

Tajni ključ je matrica S koja se bira uniformno i nasumično iz skupa $\mathbb{Z}_q^{n \times l}$. Neka su dati realan broj $\alpha > 0$ i raspodela ψ_α.

Javni ključ se dobija na sledeći način:

- bira se matrica $A \in \mathbb{Z}_q^{m \times n}$ uniformno i slučajno,
- bira se slučajno i uniformno matrica $E \in \mathbb{Z}_q^{m \times l}$ tako da je svaki elemenat izabran pomoću ψ_α,
- javni ključ je $(A, P = AS + E) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^{m \times l}$.

Šifrovanje
Ako je dat vektor $v \in \mathbb{Z}_t^l$ (poruka) i javni ključ (A, P), izabrati vektor $a \in \{-r, -r+1, ..., r\}^m$ uniformno i nasumično. Šifrovani tekst je $(u = A^T a, c = P^T a + f(v)) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^l$.

Dešifrovanje

Ako je dat šifrat $(u, c) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^l$ i tajni ključ $S \in \mathbb{Z}_q^{n\times l}$, poruka v se dobija računanjem $f^{-1}(c - S^T u)$.

Greške u dešifrovanju

Postoji mogućnost pogrešnog dešifrovanja u opisanom kriptosistemu, koja se može načiniti veoma malom s dobrim izborom parametara. Verovatnoća greške dešifrovanja jednog slova, odnosno elementa iz skupa $\mathbb{Z}_t$ procenjuje se kao što je to učinjeno u radu [3].

Neka je S tajni ključ, (A, P) javni ključ i poruka koju želimo da šifrujemo v. Rezultat je dat sa

$$\begin{aligned} f^{-1}(c - S^T u) &= f^{-1}(P^T a + f(v) - S^T A^T a) \\ &= f^{-1}((AS + E)^T a + f(v) - S^T A^T a) \\ &= f^{-1}(E^T a + f(v)). \end{aligned}$$

Da bi se desila greška u dešifrovanju, na primer u prvom slovu, onda bi prva koordinata vektora $E^T a$ morala da bude veća od $|\frac{q}{2t}|$. Kada se fiksira vektor a (i ignoriše zaokruživanje) raspodela prve koordinate vektora $E^T a$ je normalna raspodela sa srednjom vrednošću 0 i standardnom devijacijom $\frac{\alpha q \|a\|}{\sqrt{2\pi}}$, jer je suma nezavisnih slučajnih promenljivih koje imaju normalnu raspodelu opet promenljiva s normalnom raspodelom, čija je disperzija suma datih disperzija. Norma vektora a je sa velikom verovatnoćom blizu vrednosti

$$\|a\| \approx \sqrt{r(r+1)m/3}.$$

Zaista, svaka koordinata vektora a je dobijena uniformnom raspodelom na skupu $\{-r, -r+1, ..., r\}$. Stoga je očekivanje na kvadrat svake koordinate

$$\frac{1}{2r+1} \sum_{i=-r}^{r} i^2 = \frac{r(r+1)}{3},$$

te je $\|a\|^2$ vrlo blizu $r(r+1)m/3$. Sada se verovatnoća greške dešifrovanja jednog slova može proceniti kao verovatnoća da slučajna promenljiva s normalnom raspodelom čija je srednja vrednost 0, a standardna devijacija $\alpha q\sqrt{r(r+1)m/(6\pi)}$ uzme vrednost veću od $|\ \frac{q}{2t}\ |$, odnosno verovatnoća greške po slovu je približno jednaka

$$2\left(1 - \Phi\left(\frac{1}{2t\alpha}\sqrt{\frac{6\pi}{r(r+1)m}}\right)\right),$$

gde je Φ funkcija raspodele verovatnoće standardne normalne raspodele, tj. $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{1}{2}t^2} dt$.

Kriptosistem je otporan na napade odabranog otvorenog teksta, tj. CPA napade (engl. *Chosen Plaintext Attacks*) a dokaz o sigurnosti dat je u [3]. Dokaz se sastoji iz dva dela. U prvom delu pokazano je da bi razlikovanje javnog ključa (A, P), generisanog kriptosistemom, od para (A, P) koji je izabran uniformno i nasumično iz skupa $\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^{m\times l}$ impliciralo rešenje LWE problema s parametrima n, m, q, ψ_α. Stoga, ako se izaberu parametri za koje se veruje da je LWE problem težak, onda je ove parove nemoguće razlikovati. U drugom delu je dokazano da ako bi neko želeo da šifruje poruku javnim ključem (A, P) koji je izabran slučajno, onda šifrat s velikom verovatnoćom ne bi sadržao neki statistički podatak o otvorenom tekstu. U suštini, drugi deo dokaza garantuje da bi razbijanje kriptosistema podrazumevalo sposobnost razlikovanja javnog ključa od nekog uniformnog slučajnog para, što je na osnovu prvog dela dokaza veoma teško.

Praktičnost kriptosistema

Objekat	**Veličina u bitovima**
Tajni ključ	$nl \log_2 q$
Javni ključ	$m(n+l) \log_2 q$
Poruka	$l \log_2 t$
Šifrat	$(n+l) \log_2 q$
Operacija	**Vreme**
Šifrovanje	$\tilde{O}(m(1+n/l))$
Dešifrovanje	$\tilde{O}(n)$

Tabela 7: Veličine ključeva, poruke, šifrata i vreme operacija u LWE kriptosistemu.

Napomena 8. $\tilde{O}(\cdot)$ *označava da su logaritamski faktori sakriveni.*

Kris Pajkert i Brent Voters (Brant Waters) su u radu [34] predstavili kriptosistem zasnovan na LWE problemu koji je otporan na napade odabranog šifrovanog teksta, odnosno CCA napade (engl. *Chosen Ciphertext Attacks*). Da bi to ostvarili, oni su kreirali koncept *zamke s gubitkom* (engl. *lossy trapdoors*) koje se ponašaju dvojako. Mogu da budu funkcije sa zamkom, a mogu da budu funkcije koje gube dosta informacija u smislu da svaka slika ima više originala. Pokazali su da su ova dva ponašanja međusobno neraspoznatljiva. Pajkert je naknadno dao još jednu konstrukciju za CCA sigurnu kriptografsku šemu, gde koristi funkcije sa zamkama koje se sastoje od dobre baze rešetke, kreirane LWE problemom. Za više detalja, pogledati [35].

4.2 Idealne rešetke

Mićanco je 2007. godine modifikovao Ajtaijevu jednosmernu (otpornu na kolizije) funkciju tako da funkcioniše u konvolucijskom prstenu polinoma $\mathcal{R} = \mathbb{Z}[x]/\langle x^n - 1\rangle$ i pokazao kako ona pruža poboljšanje u efikasnosti, tačnije kvazi-linearne veličine ključeva $\tilde{O}(n)$ kao i brže vreme izvršavanja. On je u svom radu [36] pokazao da je modifikovana funkcija jednosmerna pod pretpostavkom da su određeni aproksimativni problemi u $n-$dimenzionalnoj *cikličnoj rešetki* teški u najtežem slučaju. Međutim ispostavilo se da funkcija ipak nije otporna na kolizije [37], ali da sa manjim izmenama jeste. To je doprinelo većem interesovanju za ispitivanje idealnih rešetaka.

Definicija 4.2.1 (Ciklična rešetka)**.** *Rešetka $L \subseteq \mathbb{Z}^n$, gde za svaki vektor $(x_1, x_2, ..., x_n) \in L$ važi da i $(x_n, x_1, x_2, ..., x_{n-1}) \in L$ naziva se ciklična rešetka.*

Kao što je razmatrano u poglavlju 3.3.1, konvolucijski prsten polinoma je prsten $\mathcal{R} = \mathbb{Z}[x]/\langle x^n - 1\rangle$, gde je $\langle x^n - 1\rangle$ ideal prstena $\mathbb{Z}[x]$ koji se sastoji od svih umnožaka od $x^n - 1$. Prethodno je spomenuto da se za svaki polinom može definisati vektor njegovih koeficijenata. Važi i obrnuto, svaki vektor $\vec{v} \in \mathbb{Z}^n$ može se posmatrati kao vektor koeficijenata nekog polinoma v, pa tako i polinoma u prstenu $\mathcal{R}$, na sledeći način

$$\vec{v} = (v_1, v_2, ..., v_n) = v_1 + v_2 x + v_3 x^2 + ... + v_n x^{n-1}. \tag{4.2}$$

Ako je $\vec{v}$ vektor ciklične rešetke L, a v njemu odgovarajući polinom, onda je i vektor koji odgovara polinomu xv takođe u njoj. Zaista,

$$\begin{aligned} xv &= x\big(v_1 + v_2 x + v_3 x^2 + ... + v_n x^{n-1}\big) \\ &= v_1 x + v_2 x^2 + v_3 x^3 + ... + v_n x^n \\ &= v_n + v_1 x + v_2 x^2 + v_3 x^3 + ... + v_{n-1} x^{n-1} \text{ u } \mathbb{Z}[x]/\langle x^n - 1\rangle. \end{aligned}$$

Mićanco i Ljubaševski[11] su u radu [37] ispitivali šta bi se desilo kada bi se umesto $x^n - 1$ koristio neki drugi polinom, koji je nesvodljiv, pošto se ispostavilo da ovaj izbor polinoma nije optimalan jer se može faktorisati na $x^n - 1 = (x - 1)(x^{n-1} + ... + x + 1)$. Ovo je dovelo do detaljnijeg ispitivanja specijalne klase rešetki, idealne rešetke.

Definicija 4.2.2 (Idealna rešetka)**.** *Rešetka koja je odgovara nekom idealu I prstena $\mathbb{Z}[x]/\langle p\rangle$, gde je $p \in \mathbb{Z}[x]$ polinom oblika $x^n + z_{n-1}x^{n-1} + ... + z_1x + z_0$, $z_i \in \mathbb{Z}$ (engl. monic polynomial) naziva se idealna rešetka. Njena baza je $L(B) = \{R_p[q]|q \in I\}$, $I \subseteq \mathbb{Z}[x]/\langle p\rangle$.*

Ovakav oblik polinoma p garantuje da redukcija po modulu p daje polinome stepena manjeg od n. Može se videti da je ciklična rešetka u stvari idealna rešetka gde je $p = x^n - 1$.

Teorema 4.2.1. *Neka je $p \in \mathbb{Z}[x]$ polinom oblika $x^n + z_{n-1}x^{n-1} + ... + z_1x + z_0$, gde $z_i \in \mathbb{Z}$, koji je nesvodljiv. Ako je $v \in \mathbb{Z}[x]/\langle p\rangle$ ne-nula polinom koji odgovara vektoru $\vec{v} \in \mathbb{Z}^n$, tada su vektori koji odgovaraju polinomima $v, xv, x^2v, ..., x^{n-1}v$ linearno nezavisni.*

Dokaz. Posmatra se linearna kombinacija vektora koji odgovaraju polinomima $v, xv, ..., x^{n-1}v$, s celobrojnim koeficijentima

$$\begin{aligned} z_0v + z_1(vx) + z_2(vx^2) + ... + z_{n-1}(vx^{n-1}) = \\ v\big(z_0 + z_1x + z_2x^2 + ... + z_{n-1}x^{n-1}\big) = v * z, \end{aligned}$$

gde je z polinom koji odgovara vektoru koeficijenata $\vec{z} = (z_0, z_1, ..., z_{n-1})$. Da bi se dokazala linearna nezavisnost vektora, treba pokazati da su koeficijenti z_i jednaki 0, za svako $i = 0, 1, ..., n - 1$, tj. da je polinom $z = 0$. Ako je $z_0v + z_1(vx) + z_2(vx^2) + ... + z_{n-1}(vx^{n-1}) = 0$, onda je $R_p[v * z] = 0$. Kako je p nesvodljiv, a $\mathbb{Z}[x]$ prsten sa jedinstvenom faktorizacijom, sledi da je p i prost elemenat u $\mathbb{Z}[x]$, odnosno ako p deli qr, onda p deli q ili r (ili oba). S obzirom na to da p deli $v * z$, imamo da p deli z ili v. Međutim, oba polinoma su stepena manjeg od n, pa kako je v ne-nula polinom, sledi da z mora biti 0. □

Iz ove teoreme sledi da je svaka (netrivijalna) idealna rešetka L kompletna, odnosno ranga n, ako je p nesvodljiv. Vektori koji odgovaraju polinomima $v, xv, ..., x^{n-1}v$ su ciklične rotacije vektora $\vec{v}$ i stoga imaju istu normu kao i vektor $\vec{v}$. Mićanco i Ljubaševski u svom radu takođe zahtevaju da za bilo koji polinom q, njegova norma u prstenu $\|q\|_p := \|R_p[q]\|_\infty$ nije puno veća od norme $\|q\|_\infty$. Oni za polinom p koji bi ispunjavao ova svojstva predlažu polinom $x^n + 1$, gde je $n = 2^k, k \in \mathbb{N}$. Slično kao u slučaju cikličnih rešetaka, množenjem nekog polinoma $v \in \mathbb{Z}[x]/\langle x^n + 1\rangle$ koji odgovara vektoru $\vec{v}$ idealne rešetke, sa x, dobijamo polinom koji odgovara cikličnoj rotaciji vektora v s malom razlikom

$$\begin{aligned} xv &= x\big(v_1 + v_2x + v_3x^2 + ... + v_nx^{n-1}\big) \\ &= v_1x + v_2x^2 + v_3x^3 + ... + v_nx^n \\ &= -v_n + v_1x + v_2x^2 + v_3x^3 + ... + v_{n-1}x^{n-1} \text{ u } \mathbb{Z}[x]/\langle x^n + 1\rangle, \end{aligned}$$

što odgovara vektoru $(-v_n, v_1, v_2, ..., v_{n-1})$. Ovaj vektor se još naziva anticiklična rotacija vektora $\vec{v}$. Na osnovu prethodne teoreme, odgovarajući vektori za polinome $v, xv, ..., x^{n-1}v$ su linearno nezavisni i imaju istu normu kao vektor $\vec{v}$.

[11] Vadim Ljubaševski, rođen 1980. godine u Ukrajini, je kriptograf u grupi bezbednosti, na odeljenju za kognitivno računarstvo i industrijska rešenja.

Kao posledica, dobija se da su SVP i SIVP problem ekvivalentni u idealnim rešetkama. Zaista, neka je v najkraći ne-nula vektor (dužine $\lambda_1(L)$) idealne rešetke L koja odgovara idealu prstena $\mathbb{Z}[x]/\langle x^n+1\rangle$. Tada, na osnovu prethodno spomenutih rezultata, nalaženje jednog najkraćeg ne-nula vektora $v \in L$ povlači nalaženje n nezavisnih najkraćih vektora $v, xv, ..., x^{n-1}v$ koji su rešenje SIVP problema (svi su dužine $\lambda_1(L)$). Obrnuto, ako vektori $v, xv, ..., x^{n-1}v$ formiraju rešenje SIVP problema, onda je $\lambda_1(L) = \lambda_2(L) = \cdots = \lambda_n(L)$, pa su ovo ujedno i rešenja SVP problema. Još jedna posledica je da problem GapSVP$_{\sqrt{n}}$ u idealnoj rešetki postaje lak. To se može videti iz naredne teoreme.

Teorema 4.2.2. *Neka je L idealna rešetka koja odgovara idealu prstena $I \subseteq \mathbb{Z}[x]/\langle x^n+1\rangle$. Tada važi*

$$\sqrt[n]{det(L)} \leq \lambda_1(L) \leq \sqrt{n}\sqrt[n]{det(L)}.$$

Kao što je definisano u poglavlju 2.2, za problem GapSVP$_{\sqrt{n}}$, gde je dat neki realan broj $r > 0$, algoritam vraća odgovor DA ako je $\lambda_1(L) \leq r$, a NE ako je $\lambda_1(L) > \sqrt{n}r$. U slučaju da je $r < \lambda_1(L) \leq \sqrt{n}r$ oba odgovora su prihvatljiva. Dakle, odgovor DA je prihvatljiv ako je $0 < \lambda_1(L) \leq \sqrt{n}r$, a NE ako je $r < \lambda_1(L)$.
Neka je $\sqrt[n]{det(L)} \leq r$. Tada je na osnovu teoreme 4.2.2

$$\lambda_1(L) \leq \sqrt{n}\sqrt[n]{det(L)} \leq \sqrt{n}r,$$

te je odgovor DA prihvatljiv. Ako je ipak $\sqrt[n]{det(L)} > r$, onda je

$$r < \sqrt[n]{det(L)} \leq \lambda_1(L),$$

pa je NE prihvatljiv odgovor. Dakle, za idealnu rešetku L problem GapSVP$_{\sqrt{n}}$ može se rešiti računanjem determinante $\sqrt[n]{det(L)}$.

Mićanco je pokazao da se na osnovu teško rešivih problema u idealnim rešetkama dobijaju dokazivo sigurne heš funkcije i jednosmerne funkcije sa zamkom, pod pretpostavkom da je redukovanje baze idealne rešetke slično redukovanju slučajne rešetke.
Demijan Stehle (Damien Stehlé) i Ron Stajnfeld (Ron Steinfeld) su u radu [38] modifikovali NTRU kriptosistem, kako bi postao dokazivo siguran, tako što su umesto konvolucijskog prstena polinoma $\mathbb{Z}[x]/\langle x^n-1\rangle$ posmatrali prsten koji su predlagali Mićanco i Ljubaševski, tj. $\mathbb{Z}[x]/\langle x^n+1\rangle$, gde je $n = 2^k, k \in \mathbb{Z}$. Dokaz se zasniva na Ring-LWE problemu za koji se veruje da je NP-težak u idealnim rešetkama.
Džintaj Ding (Jintai Ding) i Ričard Lindner (Richard Lindner) su međutim dali nagoveštaj da problemi u idealnim rešetkama ne predstavljaju generalni slučaj, tako što su izumeli algoritam koji razlikuje idealnu rešetku od one koja nije. Algoritam za vreme $O(n^4)$ odlučuje da li data baza ranga n generiše idealnu rešetku ili ne. Koristeći ovaj algoritam oni su za nekoliko dimenzija pokazali da slučajno generisane rešetke praktično nikad nisu idealne (pogledati [39]).

5 Neke primene

Sem već pomenutih primena u šifrovanju s javnim ključem, konstruisanju funkcija otpornih na kolizije i jednosmernih funkcija sa zamkom, postoje još razne primene kriptografije zasnovane na rešetkama, a neke od njih su posebno značajne jer nam omogućavaju stvari koje do sad nisu bile moguće. U ovom poglavlju biće ukratko opisane primene u digitalnim (elektronskim) potpisima, šifrovanju zasnovanom na identitetu i potpuno homomorfnom šifrovanju, a još neke od primena su: šifrovanje zasnovano na atribututima (engl. *Atribute Based Encryption*), pseudo - slučajne funkcije, nejasni prenosi tj. OT (engl. *Oblivious Transfer*), funkcionalno šifrovanje itd. Interesantno je da Google trenutno eksperimentiše sa kvantnom razmenom ključeva. Za eksperiment su zaduženi Erdem Alkim (Erdem Alkim), Leo Dukas (Léo Ducas), Tomas Popelman (Thomas Pöppelmann) i Piter Švab (Peter Schwabe) koji su osmislili kvantni algoritam za razmenu ključeva "New Hope" [40] koji se zasniva na Ring-LWE problemu.

5.1 Digitalni potpisi

Pojam digitalnog potpisa prvi su uveli Vitfild Difi (Whitfield Diffie) i Martin Helman (Martin Hellman) kao jednu od mogućih primena asimetričnih algoritama. Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke, da osigura garanciju identiteta pošiljaoca poruke, da spreči osobu od poricanja da je potpisao nešto i slično. Poruke se potpisuju tajnim ključem, a potpis se može verifikovati javnim ključem. Prve dve šeme potpisa predložene su od strane autora GGH i NTRU kriptosistema. To su GGH šema potpisa i NSS (engl. *NTRU Signature Scheme*). Nakon što je NSS šema dva puta razbijena, autori su predložili NTRUSign šemu (videti [41]) koja ima isti pristup kao i GGH šema potpisa. Neformalno, poruka m se hešuje u neku tačku, u nekoj oblasti prostora, a njen potpis je tačka rešetke koja joj blizu. Tu tačku nalazimo pomoću dobre baze rešetke. Međutim, Regev i Pong Uijen (Phong Nguyen) razbili su ove šeme. Nakon toga, Ljubaševski je u [42] predložio novu šemu digitalnog potpisa, kao i identifikacionu šemu, koje su zasnovane na problemima u idealnim rešetkama. Bezbednost prve šeme se zasniva na aproksimativnom problemu najkraćeg vektora s faktorom $\gamma = \tilde{O}(n^2)$ u modelu slučajne subrutine (engl. *random oracle model*). Sigurnost druge šeme takođe se zasniva na aproksimativnom problemu najkraćeg vektora, $\text{SVP}_{\tilde{O}(n^2)}$, ali se ne zahteva da nasumična subrutina, tj. model je standardni. Protokol je veoma efikasan i sve operacije zahtevaju vreme $\tilde{O}(n)$. Pajkert, Džentri i Vinod Vakuntanatan (Vinod Vaikuntanathan) predstavili su u radu [43] iz 2008. godine, zamke (engl. *trapdoors*) u rešetkama koje koriste u nekoliko novih kriptografskih konstrukcija. Neke od ovih konstrukcija su i šeme potpisa. Oni koriste obrazac "hešovati pa potpisati" (engl. *hash-and-sign-paradigm*) u modelu slučajne subrutine. Njihove šeme u teorijskom smislu predstavljaju instanciranje GGH i NTRUSign šeme (kao varijante GGH šeme), ali s dve bitne razlike. Prva razlika je ta da su njihove šeme bazirane na problemima za nasumične rešetke, a druga je ta da su potpisi generisani algoritmom nasumičnog dekodiranja što upravo otklanja problem zbog kojeg je GGH nesigurna (propuštanje informacija o obliku baze).

5.2 Šifrovanje zasnovano na identitetu

Šifrovanje zasnovano na identitetu ili skraćeno IBE (engl. *Identity Based Encription*) je vrsta šifrovanja gde svaki string može da bude javni ključ. Na primer, nečije ime može da posluži u tu svrhu. Tajnim ključevima upravlja neki viši autoritet koji ima glavni tajni ključ sistema. Ovakva vrsta sistema ne zahteva centralno skladište svih javnih ključeva, pošto svaki identitet služi kao javni ključ tog identiteta.

U već spomenutom radu [43], autori su između ostalog konstruisali i IBE šemu zasnovanu na LWE problemu. Da bi to ostvarili, oni su prvo opisali "dualnu" verziju Regevovog kriptosistema, gde su

uloge ključeva i šifrovanog teksta u suštini zamenjene.

Dualni kriptosistem
Kriptosistem je parametrizovan nekim $r > \sqrt{\log m}$ koji određuje diskretnu Gausovu raspodelu $D_{\mathbb{Z}^m,r}$ na skupu $\mathbb{Z}^m$ kojom se biraju tajni ključevi. Svi korisnici dele zajedničku matricu $A \in \mathbb{Z}_q^{n\times m}$ koja se bira uniformno i nasumično i koja je indeks funkcije $f_A(e) = R_q[Ae]$. Sve operacije se izvode na skupu $\mathbb{Z}_q$.

- **Tajni ključ** je vektor greške e koji se dobija raspodelom $D_{\mathbb{Z}^m,r}$.
- **Javni ključ** je $u = f_A(e) = R_q[Ae]$ koji se naziva *sindrom* od e.
- **Šifrovanje**: birati slučajno i uniformno vektor $s \in \mathbb{Z}_q^n$ i vektor $x = (x_1, x_2, ..., x_m)$ tako da je svaki x_i dobijen raspodelom χ. Zatim izračunati $p = A^T s + x \in \mathbb{Z}_q^m$. Ako je u pitanju 0, šifrovan tekst je $(p, c = \langle u, s\rangle + y)$, a ako je u pitanju 1 šifrat je $(p, c = \langle u, s\rangle + y + \lfloor \frac{q}{2} \rceil)$, gde je y dobijeno raspodelom χ.
- **Dešifrovanje**: Za bilo koji par (p, c) izračunati $R_q[c - \langle e, p\rangle]$. Šifrat se dešifruje kao nula ako je rezultat bliži 0 ili q nego što je $\frac{q}{2}$, a kao jedinica inače.

Jedna prednost ovog sistema je ta da su šifrati sada LWE uzorci, a mogućnost njihovog razlikovanja od uniformnih parova je ekvivalentna rešavanju LWE odlučujućeg problema. Autori su dokazali da je ovaj sistem siguran protiv napada odabranog otvorenog teksta, kao i da je anoniman, u smislu da nije moguće videti kojim je javnim ključem šifrovana poruka, što se smatra poželjnim svojstvom za enkripciju zasnovanu na identitetu.

Da bi ovaj sistem pretvorili u IBE šemu, autori koriste njihove konstrukcije sa zamkama. Tačnije, oni vezuju identitete za javne ključeve u koristeći slučajnu subrutinu. Da bi izračunali tajni ključ $e = f_A^{-1}(u)$ oni koriste "pre-image sampler" sa informacijom zamke, odnosno dobrom bazom koja odgovara LWE rešetki. Postupci šifrovanja i dešefrovanja vrše se kao u opisanom dualnom kriptosistemu. Za detaljniji opis ove šeme pogledati [43].

5.3 Potpuno homomorfno šifrovanje

Kao što je spomenuto u uvodu, homomorfno šifrovanje predstavlja sposobnost izvođenja operacija nad šifratima, bez poznavanja odgovarajućeg otvorenog teksta. Specijalno, ono omogućava da se šifrat poruke m transformiše u šifrat bilo koje funkcije $f(m)$ bez poznavanja tajnog ključa. Potpuno homomorfna enkripcijska šema omogućava operacije sabiranja i množenja. Postojanje ovakve šeme bilo je otvoreno pitanje u kriptografiji, sve dok Kreg Džentri nije predstavio prvu potpuno homomorfnu šemu u svom radu [44] koristeći idealne rešetke. Međutim, pošto šema nije veoma praktična, usledile su neke optimizacije (na primer [45]). Prvu implementaciju Džentrijeve šeme dali su Nigel Smart (Nigel Smart) i Frederik Verkauteren (Frederik Vercauteren), koristeći takođe idealne rešetke, iako nisu bili implementirani svi aspekti šeme. Džentri i Halevi su nakon toga implementirali šemu sa dodatnim optimizacijama, tako da su svi aspekti šeme uključeni. Međutim, parametri i dalje nisu bili skroz praktični, zbog velikih javnih ključeva (70 megabajta - 2.3 gigabajta) koji zavise od dimenzije rešetke (videti [46]). Zvika Brakerski (Zvika Brakerski) i Vinod Vakuntanatan pružili su "drugu" generaciju potpuno homomorfnih enkripcijskih konstrukcija, zasnovanih na LWE problemu [47].

6 Zaključak

Kriptografija zasnovana na rešetkama je relativno nova oblast koja se pak razvija velikom brzinom. Ona nam pruža efikasne i sigurne kriptosisteme koji će to svojstvo zadržati i s pojavom kvantnih računara, za razliku od asimetričnih kriptosistema koji se danas koriste. Postoje mnoge njene primene, a novine koje nam ova oblast donosi razlog su više za njeno korišénje u praksi. Postoje još mnoga otvorena pitanja kao na primer da li je moguće dokazati da su određeni problemi u rešetkama teški i u idealnim. Ako nije, da li je moguće osmisliti nove probleme koji jesu? Da li postoji klasična redukcija GapSVP_γ i SIPV_γ problema na LWE problem, umesto Regevove kvantne redukcije? To su samo neki od, za sada, nerešenih problema, a kako se oblast vrlo brzo širi, što je više odgovora, to je više novih pitanja. Upravo to je ono što je najlepše, mogućnost neprekidnog izučavanja, bez bojazni da će u skorije vreme većina informacija biti otkrivena.

7 Literatura

[1] Ronald L Rivest, Len Adleman, and Michael L Dertouzos. On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11):169–180, 1978.

[2] Joseph H. Silverman Jeffrey Hoffstein, Jill Pipher. *An Introduction to Mathematical Cryptography*. Springer, 2008.

[3] Daniele Micciancio and Oded Regev. Lattice-based cryptography. In *Post-quantum cryptography*, pages 147–191. Springer, 2009.

[4] Miklós Ajtai. Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 99–108. ACM, 1996.

[5] Johannes Blömer and Jean-Pierre Seifert. On the complexity of computing short linearly independent vectors and short bases in a lattice. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 711–720. ACM, 1999.

[6] Yi-Kai Liu, Vadim Lyubashevsky, and Daniele Micciancio. On bounded distance decoding for general lattices. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 450–461. Springer, 2006.

[7] Irit Dinur, Guy Kindler, Ran Raz, and Shmuel Safra. Approximating cvp to within almost-polynomial factors is np-hard. *Combinatorica*, 23(2):205–243, 2003.

[8] Subhash Khot. Hardness of approximating the shortest vector problem in lattices. *Journal of the ACM (JACM)*, 2004.

[9] Martin Henk. Note on shortest and nearest lattice vectors. *Information Processing Letters*, 61 (4):183–188, 1997.

[10] Oded Goldreich, Daniele Micciancio, Shmuel Safra, and J-P Seifert. Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. *Information Processing Letters*, 71(2):55–61, 1999.

[11] Daniele Micciancio and Shafi Goldwasser. *Complexity of lattice problems: a cryptographic perspective*, volume 671. Springer Science & Business Media, 2012.

[12] Peter Borwein. *Computational excursions in analysis and number theory*. Springer Science & Business Media, 2012.

[13] Miklós Ajtai. The shortest vector problem in l 2 is np-hard for randomized reductions. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 10–19. ACM, 1998.

[14] Daniele Micciancio. Improving lattice based cryptosystems using the hermite normal form. In *Cryptography and Lattices*, pages 126–145. Springer, 2001.

[15] J.H. van de Pol. Lattice-based cryptography. *Master's thesis, Eindhoven University of Technology*, 2011.

[16] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Public-key cryptosystems from lattice reduction problems. In *Annual International Cryptology Conference*, pages 112–131. Springer, 1997.

[17] Daniele Micciancio. Improving lattice based cryptosystems using the hermite normal form. In *Cryptography and Lattices Conference — CaLC 2001*, volume 2146 of *Lecture Notes in Computer Science*, Providence, Rhode Island, 2001. Springer-Verlag.

[18] J. Pipher J. Hoffstein and J. Silverman. A new high speed public key cryptosystem, algorithmic number theory. *Lecture Notes in Computer Science*, pages 267–288, 1998.

[19] Z Milan Grulović. *Osnovi teorije grupa*. Institut za matematiku u Novom Sadu, 1997.

[20] NTRU Cryptosystems. The ntru public key cryptosystem-a tutorial, 1998.

[21] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. Ntru: A ring-based public key cryptosystem. In *International Algorithmic Number Theory Symposium*, pages 267–288. Springer, 1998.

[22] Nick Howgrave-Graham, Joseph H Silverman, Ari Singer, William Whyte, and NTRU Cryptosystems. Naep: Provable security in the presence of decryption failures. *IACR Cryptology ePrint Archive*, page 172, 2003.

[23] William Whyte, Nick Howgrave-Graham, Jeffrey Hoffstein, Jill Pipher, Joseph H Silverman, and Philip S Hirschhorn. Ieee p1363. 1 draft 10: Draft standard for public key cryptographic techniques based on hard problems over lattices. *IACR Cryptology ePrint Archive*, page 361, 2008.

[24] John Proos. *Imperfect decryption and an attack on the NTRU encryption scheme*. Faculty of Mathematics, University of Waterloo, 2003.

[25] Oded Regev. New lattice-based cryptographic constructions. *Journal of the ACM (JACM)*, 51 (6):899–942, 2004.

[26] Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 284–293. ACM, 1997.

[27] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. 2005.

[28] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 333–342. ACM, 2009.

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

[30] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. In *SIAM J. on Computing*, 2004.

[31] Daniele Micciancio and Chris Peikert. Hardness of sis and lwe with small parameters. In *Advances in Cryptology–CRYPTO 2013*, pages 21–39. Springer, 2013.

[32] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 1–23. Springer, 2010.

[33] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In *Annual International Cryptology Conference*, pages 554–571. Springer, 2008.

[34] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. 2008.

[35] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 333–342. ACM, 2009.

[36] Daniele Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Computational Complexity*, 16(4):365–411, 2007.

[37] Vadim Lyubashevsky and Daniele Micciancio. Generalized compact knapsacks are collision resistant. In *International Colloquium on Automata, Languages, and Programming*, pages 144–155. Springer, 2006.

[38] Damien Stehlé and Ron Steinfeld. Making ntru as secure as worst-case problems over ideal lattices. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 27–47. Springer, 2011.

[39] Jintai Ding and Richard Lindner. Identifying ideal lattices. *IACR Cryptology ePrint Archive*, 2007:322, 2007.

[40] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange-a new hope. Technical report, Cryptology ePrint Archive, Report 2015/1092, 201 5. http://eprint. iacr. org, 2015.

[41] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H Silverman, and William Whyte. Ntrusign: Digital signatures using the ntru lattice. In *CryptographersâĂŹ Track at the RSA Conference*, pages 122–140. Springer, 2003.

[42] Vadim Lyubashevsky. Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 598–616. Springer, 2009.

[43] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008.

[44] Craig Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009.

[45] Damien Stehlé and Ron Steinfeld. Faster fully homomorphic encryption. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 377–394. Springer, 2010.

[46] Craig Gentry and Shai Halevi. Implementing gentry's fully-homomorphic encryption scheme. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 129–148. Springer, 2011.

[47] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) lwe. *SIAM Journal on Computing*, 43(2):831–871, 2014.

Biografija

Jovana Vajagić rođena je u Rumi, 26.10.1992. godine. Osnovne akademske studije završila je 2015. god. na Prirodno-matematičkom fakultetu u Novom Sadu i stekla zvanje diplomirani profesor matematike. Nakon toga upisuje se na Fakultet tehničkih nauka, smer matematika u tehnici. Sve ispite položila je u roku, sa prosečnom ocenom 9.5 i time stekla uslov za odbranu master rada.