Univerzitet u Beogradu
Matematički fakultet

Master rad

Kriptografija zasnovana na rešetkama

Mentor:
Prof. dr Goran Đanković

Student:
Ana Radivojević 1072/2020

Beograd, 2023.

Sadržaj

Spisak slika

Spisak tabela

1. Uvod

1.1 Kratki uvod u kriptografiju

Kroz istoriju je postojala potreba da se omogući komunikacija između dve ili više strana, a da se zadrži privatnost informacija koje se prenose, naročito u slučaju kada postoji prisluškivanje komunikacionog kanala. Sa tom potrebom je nastala kriptografija.

Dok je obezbeđivanje privatnosti ostao glavni cilj, polje kriptografije je prošireno na niz drugih oblasti, ne samo u okviru bezbednosti komunikacije, kao što su integritet i autentičnost komunikacija, već i na mnoge druge sofisticiranije ciljeve.

Danas je kriptografija široko rasprostranjena iako je nekada bila primenjivana uglavnom u vojne svrhe. U elektronskom bankarstvu se kriptografija koristi da bi se obezbedio pristup ličnim podacima i transakcijama. Na primer, pri kupovini preko Interneta upravo se kriptografija koristi da bi se osigurala privatnost broja platne kartice dok se prenosi od korisnika do servera prodavnice.

Kriptografija se koristi skoro od kada postoje pisani zapisi. Većim delom svoje istorije, kriptografija je bila umetnost, igra maštovitih rešenja i napada. Iako je zadržala neke od svojih starih čari, poslednjih tridesetak godina je donelo nešto sasvim novo. Umetnost kriptografije je spojena sa naukom, a danas govorimo o modernoj kriptografiji. Danas je kriptografija temelj računarske i komunikacione tehnologije. Zasniva se na strogim matematičkom principima i spaja oblasti kao što su teorija brojeva, teorija računarske kompleksnosti i teorija verovatnoće.

1.2 Opšti pojmovi u kriptografiji

Kriptologija (engl. *cryptology*) je oblast matematike koja obuhvata i kriptografiju i kriptoanalizu.

Kriptografija (engl. *cryptography*) je veština i nauka čuvanja bezbednosnih poruka. Naziv kriptografija potiče od grčke reči ***kriptos***, što znači skriven. Ona omogućava da subjekt A (pošiljalac) sigurno pošalje svoju poruku subjektu B (primaocu), tako da nepoznata treća strana, subjekt C (napadač) ne može da dođe do njenog sadržaja.

Kako bi pojednostavili izražavanje i lakše formulisali različite scenarije koji se javljaju

u radu, uvešćemo jedan broj apstraktnih subjekata ili *likova* sa određenom ulogom u procesu razmene poruka. Glavni likovi u kriptografskom scenariju su Alisa, Bob i Eva. Alisa i Bob razmenjuju tajne poruke.

Poruka koja se šalje naziva se još i ***otvoreni tekst*** (engl. *plaintext*). To je informacija u bilo kom obliku (tekstualni dokument, niz bitova, digitalni zapis,...)

Šifrovanje (engl. *encryption*) je proces maskiranja poruke, koji za cilj ima skrivanje njenog sadržaja. Šifrovana poruka se ***šifrat*** (engl. *ciphertext*).

Dešifrovanje (engl. *decryption*) je proces vraćanja šifrovane poruke u otvoreni tekst.

Označimo otvoreni tekst sa P, šifrat sa C, funkciju šifrovanja sa E, funkciju dešifrovanja sa D. Proces šifrivanja poruke matematički se zapisuje:

$$E(P) = C, \tag{1.1}$$

a dešifrovanje šifrata

$$D(C) = P. \tag{1.2}$$

Kako je cilj šifrovanja i dešifrovanja prenošenje originalne poruke, treba da važi

$$D\big(E(P)\big) = P. \tag{1.3}$$

Kriptografski algoritam, poznat kao ***šifra*** (engl. *cipher*) je matematička funkcija koja se koristi za šifrovanje i dešifrovanje (u osnovi su to dve srodne funkcije: jedna za šifrovanje, druga za dešifrovanje).

Kriptoanaliza (engl. *cryptanalysis*) je nauka razbijanja i čitanja šifrovanih poruka. Pokušaj kriptoanalize naziva se ***napad***. Uspešna kriptoanaliza naziva se ***dekriptiranje***. Cilj kriptoanalize je pronalaženje slabosti date kriptografske šeme u cilju njenog razbijanja.

Kriptoanaliza se preduzima od strane zlonamernih napadača sa ciljem obaranja sistema ili od strane samih dizajnera, radi provere sigurnosti i eventualne ranjivosti sistema. U tom smislu, cilj kriptoanalize ne mora obavezno biti obaranje sistema i otkrivanje sadržaja skrivene poruke.

1.3 Cilj kriptografije

Idealni komunikacioni kanal. Zamislimo naše dve strane kako komuniciraju kroz neprobojnu i zvučno nepropustivu cev kroz koju pošiljalac može da šapne poruku, a primalac da je čuje. Niko drugi ne može da čuje razgovor niti da izmeni bilo šta u njemu. Ova cev predstavlja savršeni komunikacioni kanal, dostupan samo onome ko šalje i onome ko prima poruku, kao da su sami na svetu. Sa stanovišta bezbednosti ovaj komunikacioni kanal je idealan.

Osnovni cilj kriptografije jeste da omogući komunikaciju koja ima slična svojstva sa idealnim komunikacionim kanalom. Kriptografija treba da obezbedi:

1. ***Tajnost podataka*** obezbeđuje da je sadržaj informacije dostupan samo ovlašćenim osobama, tj. samo onima koji poseduju ključ. Postoji više načina zaštite tajnosti, počev od fizičke zaštite do matematičkih algoritama koji podatke čine nerazumljivim.

2. ***Integritet podataka*** brine o tome da ne dođe do manipulacije ili promene podataka, kao što su brisanje i zamena podataka. Da bi se obezbedio integritet podataka, mora postojati mogućnost provere da li je informacija promenjena od strane neovlašćene osobe ili ne.

3. ***Autentičnost*** omogućava identifikaciju pošiljaoca i primaoca, tj. omogućava obema stranama proveru porekla poruke. Poruka koja se prenosi preko kanala mora biti verna originalu, da se utvrdi sadržaj, vreme slanja itd. Zbog toga i postoji podela klasa potvrde i autentičnosti podataka originalu.

4. ***Neporecivost ili neodricanje*** podrazumeva da se poslata poruka ne može negirati po bilo kom osnovu: kako po pitanju samog sadržaja, tako i po pitanju identiteta osobe koja je poruku poslala. To je vrlo važna stavka, posebno u današnje vreme kada se veliki deo novčanih i ostalih raznovrsnih transakcija obavlja putem Interneta.

2. Kriptosistemi

Ukoliko je sigurnost informacije zasnovana na tajnosti korišćenog algoritma za šifrovanje, radi se *ograničenim* (engl. *restricted*) algoritmima [1].

Nedostatke ograničenih algoritama savremena kriptografija rešava korišćenjem ***ključa*** (engl. *key*) za šifrovanje i dešifrovanje. Označimo ga sa K. Sigurnost ovih algoritama zasniva se na tajnosti ključa i ne zavisi od detalja algoritma šifrovanja. Napadač, iako je upoznat sa algoritmom korišćenim za šifrovanje, neće moći da otkrije sadržaj poruke bez poznavanja ključa kojim je poruka šifrovana.

Funkcije šifrovanja i dešifrovanja ovih algoritama zavise od izbora ključa, pa se mogu zapisati:

$$\begin{aligned} E_K(P) &= C \\ D_K(C) &= P \end{aligned} \tag{2.1}$$

i za njih važi

$$D_K\big(E_K(P)\big) = P. \tag{2.2}$$

Kriptosistem (engl. *cryptosystem*) predstavlja algoritam sa svim mogućim otvorenim tekstovima, ključevima i šiframa.

Zaštita šifrovanih poruka zavisi od zaštite ključa, a ne od zaštite algoritma. U zavisnosti od načina korišćenja ključa, razvile su se dve klase algoritama. Jedna je simetrična klasa, a druga je asimetrična klasa.

2.1 Simetrični kriptosistemi

Osnovna osobina simetričnih kriptosistema je da se za enkripciju i dekripciju poruka koristi **isti ključ**. Jedan od osnovnih problema ovakvih kriptosistema je kako uspostaviti zajednički ključ između Alise i Boba. Dakle, potreban je neki oblik *sigurnog* komunikacionog kanala preko koga bi u nekoj, početnoj fazi, dva subjekta koja komuniciraju uspostavila zajednički ključ.

Najpoznatiji algoritmi simetričnih kriptosistema koji se danas koriste su: **DES**, **3DES**,

[1] Ograničen algoritam je algoritam za izračunavanje matematičke funkcije sa ograničenjima na opseg argumenta ili preciznost zahtevanu u rezultatu.

DES-CBC, **IDEA**, **RC5**, **RC6**, **AES** i drugi.

Problemi simetričnih kriptosistema su:

- Ključevi se moraju distribuirati u tajnosti. Sigurnost ovih algoritama zasniva se na tajnosti ključa i oni su vredni koliko i poruke koje šifruju, jer poznavanje ključa daje uvid u sve poruke.

- Napadač može da se pretvara da je jedan od učesnika u komunikaciji i da proizvodi lažne poruke koje bi se šifrovale tim ključem. Jednom otkriveni ključ može da dešifruje sve poruke koje su njime šifrovane.

- Ukoliko svaki par korisnika u mreži upotrebljava poseban ključ, ukupan broj ključeva se uvećava sa rastom broja korisnika. Tako je npr. za mrežu od n korisnika potrebno $n(n-1)/2$ ključeva. Ovaj problem se može minimizirati tako što bi broj korisnika u mreži bio mali, ali to nije uvek moguće.

2.2 Asimetrični kriptosistemi

Može se reći da su Vitfild Difi [2] i Martin Helman [3] dali ključan doprinos u razvoju asimetrične kriptografije, kada su 1976. godine u svom radu *"New Direction in Cryptography"* opisali ideju kriptografije koja se temelji na dva ključa, tajnom i javnom ključu. Ova dva naučnika su potom napravili konkretan algoritam sigurne razmene ključeva, a 1977. godine Rivest [4], Šamir [5] i Adleman [6] su realizovali i patentirali čuveni **RSA** algoritam.

U literaturi pojam asimetrične enkripcije se poistovećuje sa terminom *asymmetric-key* ili *public-key* enkripcijom.

Algoritmi sa javnim ključem osmišljeni su tako da se za šifrovanje i dešifrovanje koriste različiti ključevi. Ključ za dešifrovanje ne može biti (bar ne u razumnom vremenskom roku [7]) izveden od ključa za šifrovanje. Stoga je čest slučaj da je ključ za šifrovanje javan i poznat svima, a samo strana koja ima odgovarajući ključ za dešifrovanje može doći do poruke. Ovaj postupak liči na korišćenje poštanskog sandučeta. Ubacivanje pošte u sanduče analogno je šifrovanju pomoću javnog ključa - svako to može da učini. Uzimanje pošte iz sandučeta analogno je dešifrovanju pomoću privatnog ključa - samo vlasnik sandučeta to

[2] *Whitfield Diffie* (1944) je američki kriptograf i matematičar i jedan od pionira kriptografije "javni ključ" (public-key) zajedno sa Martinom Helmanom. Dobitnik je Tjuringove nagrade.

[3] *Martin Hellman* (1945) je američki kriptograf i matematičar, najpoznatiji po svom radu sa Vitfildom Difijem na kriptografiji javnog ključa. Zajedno sa Difijem dobio je prestižnu Tjuringovu nagradu 2015. godine.

[4] *Ron Rivest* (1947) je američki kriptograf i informatičar čiji rad obuhvata oblasti algoritama, kombinatorike, kriptografije i mašinskog učenja. Uz Šamira i Adlemana jedan je od pronalazača RSA algoritma.

[5] *Adi Shamir* (1952) je izraelski kriptograf koji je u saradnji sa Rivestom i Adlemanom izumitelj RSA algoritma. Jedan je od pronalazača diferencijalne kriptoanalize.

[6] *Leonard Adleman* (1945) je američki programer i jedan od kreatora RSA kriptografskog algoritma. Dobitnik je Tjuringove nagrade.

[7] Ukoliko je vreme potrebno za razbijanje šifre duže od vremena tokom kojeg je neophodno da šifrovani podaci ostanu tajna, algoritam se smatra bezbednim.

može elegantno da uradi.

Ovaj postupak je matematički zasnovan na **jednosmernim funkcijama sa zamkom** (engl. *trapdoor one-way function*). One su zasnovane na pojmu **jednosmernih funkcija** (engl. *one-way function*). To su funkcije koje je relativno lako izračunati, ali je mnogo teže naći inverznu funkciju. Dobar primer jednosmerne funkcije jeste razbijanje tanjira - jednostavno je smrskati tanjir na hiljadu delova, ali nije nimalo lako ponovo ga sastaviti.

Matematički primer jednosmerne funkcije: Lako je naći proizvod dva prosta broja, a teško je posle taj broj rastaviti na proste činioce.

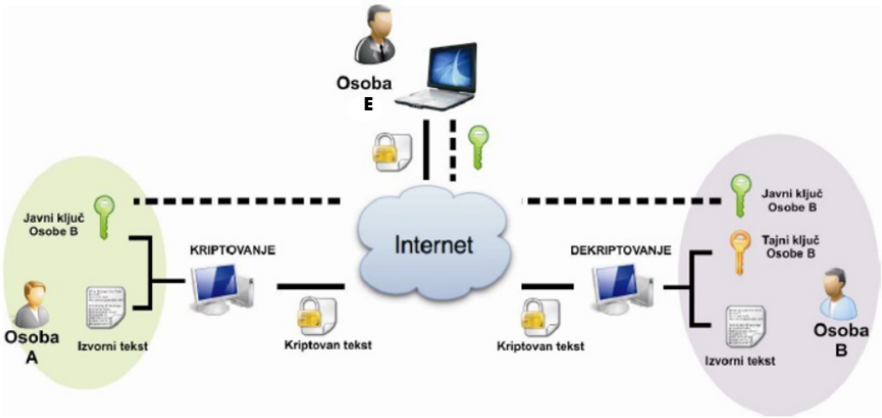
Jednosmerne funkcije sa zamkom su poseban tip jednosmernih funkcija, sa skrivenom zamkom. Izračunavanje u jednom smeru je i dalje jednostavno, ali je teško nalaženje inverzne funkcije. Međutim, ukoliko znate tajnu informaciju (zamku) lako se može izračunati i drugi smer.

Često korišćeni asimetrični algoritmi: **RSA**(Rivest-Shamir-Adleman), **DH**(Diffie-Hellman), **EG**(El Gamal), **R**(Rabin), **EC**(Eliptic Curves), itd.

RSA algoritam koristi faktorisanje velikih prostih brojeva kao one-way funkciju dok **DH** koristi problem rešavanja diskretnog logaritma. Oba problema su teška, ali nikada nije bezuslovno dokazano da ne postoji efikasan algoritam koji omogućava rešavanje problema u polinomijalnom vremenu.

2.2.1 Postupak asimetrične enkripcije

Sledeći primer komunikacije između Alise i Boba može da se odvija putem bilo kojeg medija, telefona ili čak pisanih poruka, iako bi danas najverovatnije koristili Internet (videti sliku 2.1). Ako Bob želi da prima poruke šifrovane javnim ključem, on prvo generiše svoj privatni ključ koji je poznat samo njemu. Zatim generiše javni ključ, na osnovu svog privatnog ključa, i objavljuje javni ključ svim zainteresovanim stranama. Alisa koristi Bobov javni ključ da šifruje svoju poruku, šalje je Bobu koji poruku dešifruje svojim privatnim ključem. Moguće je da Alisa takođe generiše svoj privatni ključ koji deli sa Bobom. Na ovaj način oni bez prethodne definisane zajedničke tajne razmenjuju određene poruke na siguran način kroz neki javni kanal za komunikaciju.



Slika 2.1: Postupak asimetričnog kriptovanja

U realnoj situaciji mogu se prepoznati dve faze u komunikaciji između Alise i Boba. U prvoj fazi komunikacije, oni koriste public-key šifarski sistem kao što je RSA ili (EC) DH da bi se pripremila sigurna komunikacija. Alisa i Bob u ovoj fazi razmenjuju određene podatke koristeći javni i privatni ključ preko otvorenog kanala kako bi oboje na početku dogovorili parametre simetričnog šifarskog sistema koji će da koriste (npr. AES/DES/3DES) i razmenili odgovarajući zajednički tajni ključ. Nakon toga počinje druga faza komunikacije putem simetričnog šifarskog sistema korišćenjem izabranog tajnog ključa koji traje sve dok neka od strana poželi da prekine komunikaciju ili eventualno promeni parametre ili generiše novi tajni ključ. U tom slučaju ponavlja se prva faza komunikacije.

3. Kongruentni kriptosistem

U ovom poglavlju mi opisujemo model pravog kriptosistema sa javnim ključem. Ispostavlja se da ova verzija ima neočekivane veze sa rešetkama dimezije 2 i, otuda fatalnu ranjivost, pošto je dimezija tako niska.

Alisa bira veliki pozitivni ceo broj q, koji je javni parametar i dva druga cela broja f i g, koji zadovoljavaju

$$f < \sqrt{\frac{q}{2}}, \quad \sqrt{\frac{q}{4}} < g < \sqrt{\frac{q}{2}} \quad \text{i } \operatorname{nzd}(f,q) = 1 \text{ i } \operatorname{nzd}(f,g) = 1$$

i računa

$$h \equiv f_q^{-1} g \pmod{q},$$

gde je $0 < h < q$. Primetimo da su f i g mali brojevi u poređenju sa q, jer su oni $\mathcal{O}(\sqrt{q})$.

Alisin privatni ključ je par brojeva (f, g), dok je javni ključ broj h. Bob bira otvoreni tekst m i slučajan ceo broj r koji zadovoljavaju

$$0 < m < \sqrt{\frac{q}{4}} \quad \text{i} \quad 0 < r < \sqrt{\frac{q}{2}},$$

a zatim računa šifrat

$$e \equiv rh + m \pmod{q}, \text{ gde je } 0 < e < q,$$

koji šalje Alisi.

Alisa vrši dekripciju poruke računanjem prvo

$$a \equiv fe \pmod{q}, \text{ gde je } 0 < a < q,$$

a onda i računanjem

$$b \equiv f_g^{-1} a \pmod{g},$$

gde je $0 < b < g$.

Kao rezultat dobijamo $b = m$, što znači da je Alisa zaista primila Bobovu poruku m. Prvo što možemo da zapazimo je da a zadovoljava

$$a \equiv fe \equiv f(rh + m) \equiv frf_q^{-1} g + fm \equiv rg + fm \pmod{q}.$$

Ograničenje veličina na f, g, r i m povlači da je ceo broj $rg + fm$ mali,

$$rg + fm < \sqrt{\frac{q}{2}}\sqrt{\frac{q}{2}} + \sqrt{\frac{q}{2}}\sqrt{\frac{q}{4}} < q.$$

Dakle, kada Alisa izračuna $a \equiv fe \pmod{q}$, gde je $0 < a < q$ dobija tačnu vrednost

$$a = rg + fm. \tag{3.1}$$

Ovo je ključna stvar: izraz (3.1) je jednakost celih brojeva, a ne samo brojeva kongruentnih modulo q. Na kraju, Alisa računa

$$b \equiv f_g^{-1}a \equiv f_g^{-1}(rg + fm) \equiv f_g^{-1}fm \equiv m \pmod{g},$$

gde je $0 < b < g$. Kako je $m < \sqrt{\frac{q}{4}} < g$, sledi da je $b = m$.

Kongruentni kriptosistem je sumiran u sledećoj Tabeli 3.1.

Alisa	**Bob**
Kreiranje ključa	
Odabrati veliki ceo broj q. Odabrati tajne cele brojeve f i g, sa $f < \sqrt{q/2}$, $\sqrt{q/4} < g < \sqrt{q/2}$ i $\text{nzd}(f, g) = 1$ i $\text{nzd}(f, q) = 1$. Izračunati $h \equiv f_q^{-1}g \pmod{q}$. Objaviti javni ključ (q, h).	
Enkripcija	
	Odabrati prost tekst m sa $m < \sqrt{q/4}$. Koristiti Alisin javni ključ (q, h) da se izračuna $e \equiv rh + m \pmod{q}$. Poslati Alisi šifrovan tekst e.
Dekripcija	
Izračunati $a \equiv fe \pmod{q}$ sa $0 < a < q$. Izračunati $b \equiv f_g^{-1}a \pmod{g}$ sa $0 < b < g$. Onda je b izvorni tekst m.	

Tabela 3.1: Kongruentni kriptosistem sa javnim ključem

Kako Eva može da napadne ovaj sistem? Jedan način je primenom grube sile (brute-force), da traži sve moguće privatne ključeve ili sve moguće poruke, ali ovo zahteva previše operacija. Razmotrićemo Evin zadatak, koji se odnosi na nalaženje privatnog ključa (f, g) iz poznatog javnog ključa (q, h).

Nije teško uočiti da Eva može da nađe bilo koji par pozitivnih celih brojeva F i G koji zadovoljavaju

$$Fh \equiv G \pmod{q}, F = \mathcal{O}(\sqrt{q}), G = \mathcal{O}(\sqrt{q}).$$

Tada (F, G) može poslužiti kao ključ za dekripciju.

Prepisujući kongruenciju u obliku $Fh = G + qR$, preformulisaćemo Evin zadatak kao uporedo traženje para malih celih brojeva (F, G) sa osobinom da je $F(1, h) - R(0, q) = (F, G)$. Naravno, Eva zna koje su vrednosti vektora $\boldsymbol{v_1} = (1, h)$ i $\boldsymbol{v_2} = (0, q)$, od kojih je svaki dužine $\mathcal{O}(q)$ i želi da nađe linearnu kombinaciju $\boldsymbol{w} = a_1\boldsymbol{v_1} + a_2\boldsymbol{v_2}$ tako da $\boldsymbol{w}$ bude dužine $\mathcal{O}(\sqrt{q})$.

Kasnije ćemo videti u teoriji rešetki da je Evin zadatak da nađe kratki nenulti vektor u skupu vektora $L = \{a_1\boldsymbol{v_1} + a_2\boldsymbol{v_2} : a_1, a_2 \in \mathbb{Z}\}$, pod uslovom da su koeficijenti a_1 i a_2 celi brojevi. Na nesreću po Alisu i Boba postoji ekstremno brz metod za nalaženje kratkog vektora u 2-dimenzionalnoj rešetki.

3.1 Primer

Alisa bira vrednosti za q, f i g

$$q = 122430513841,\ f = 231231 \text{ i } g = 195698.$$

Ovde su $f \approx 0.66\sqrt{q}$ i $g \approx 0.56\sqrt{q}$ dopustive vrednosti. Kako je q prost broj, ispunjen je uslov $\text{nzd}(f, q) = 1$ tako da Alisa može da izračuna f_q^{-1}. Ona nalazi f_q^{-1} Euklidovim algoritmom. Rešavanjem

$$122430513841x + 231231y = 1$$

u celim brojevima, ona dobija rezultat

$$y = 122430513841n + 49194372303 \quad \text{za } n \in \mathbb{Z}.$$

Odatle dobija da je $f_q^{-1} = 49194372303 \pmod q$.

$$f_q^{-1} \equiv 49194372303 \pmod q \quad \text{i} \quad h \equiv f_q^{-1}g \equiv 39245579300 \pmod q.$$

Alisin javni ključ je par (q, h) sa vrednostima $(q, h) = (122430513841, 39245579300)$.

Bob je odlučio da pošalje Alisi otvoreni tekst $m = 123456$ koristeći nasumičnu vrednost $r = 101010$. On koristi Alisin javni ključ da izračuna šifrat

$$e \equiv rh + m \equiv 18357558717 \pmod q$$

koji šalje Alisi.

Da bi dešifrovala e Alisa prvo koristi svoju tajnu vrednost f da izračuna

$$a \equiv fe \equiv 48314309316 \pmod q.$$

(Može se uočiti da je $a = 48314309316 < 122430513841 = q$). Ona zatim koristi vrednost $f_g^{-1} \equiv 193495 \pmod g$ da izračuna

$$f_g^{-1}a \equiv 193495 \cdot 48314309316 \equiv 123456 \pmod g,$$

a ovo je, kao što je predviđeno teorijom, Bobov izvorni tekst m.

4. Rešetke

Pre nego što počnemo priču o rešetkama, treba da se prisetimo nekih važnih definicija iz linearne algebre. Vektorski prostori se mogu definisati uopšteno, ali u ovom radu će biti razmatrani samo vektorski prostori sadržani u $\mathbb{R}^m$ za neki pozitivni ceo broj m.

Vektorski prostori. Vektorski prostor V je potprostor prostora $\mathbb{R}^m$ sa vrednostima

$$\alpha_1 \boldsymbol{v_1} + \alpha_2 \boldsymbol{v_2} \in V \quad \text{za sve } \boldsymbol{v_1}, \boldsymbol{v_2} \in V \text{ i sve } \alpha_1, \alpha_2 \in \mathbb{R}.$$

Ekvivalentno, vektorski prostor je potprostor od $\mathbb{R}^m$ koji je zatvoren za sabiranje i skalarno množenje elemenata iz $\mathbb{R}$, tj. vektorski prostor je svaki skup koji je zatvoren za linearne kombinacije, odnosno koji sadrži svaku linearnu kombinaciju svojih elemenata.

Linearna kombinacija. Neka su $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_k} \in V$. Linearna kombinacija vektora $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_k} \in V$ je bilo koji vektor oblika

$$\boldsymbol{w} = \alpha_1 \boldsymbol{v_1} + \alpha_2 \boldsymbol{v_2} + \cdots + \alpha_k \boldsymbol{v_k} \quad \text{sa} \quad \alpha_1, \ldots, \alpha_k \in \mathbb{R}.$$

Suma takvih linearnih kombinacija

$$\{\alpha_1 \boldsymbol{v_1} + \cdots + \alpha_k \boldsymbol{v_k} : \alpha_1, \ldots, \alpha_k \in \mathbb{R}\},$$

se zove linearni omotač $\{\boldsymbol{v_1}, \ldots, \boldsymbol{v_k}\}$.

Nezavisnost. Skup vektora $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_k} \in V$ je linearno nezavisan skup ako je

$$\alpha_1 \boldsymbol{v_1} + \alpha_2 \boldsymbol{v_2} + \cdots + \alpha_k \boldsymbol{v_k} = 0, \tag{4.1}$$

ako i samo ako su $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$. Skup je linearno zavisan ako u jednačini (4.1) ima bar jedan koeficijent α_i različit od nule.

Baza. Baza vektorskog prostora V je skup linearno nezavisnih vektora $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}$ koji čine linearni omotač, odnosno to je svaki linearno nezavisan i generatorski skup. To je svaki vektor $\boldsymbol{w} \in V$ oblika

$$\boldsymbol{w} = \alpha_1 \boldsymbol{v_1} + \alpha_2 \boldsymbol{v_2} + \cdots + \alpha_n \boldsymbol{v_n}$$

sa jedinstvenim koeficijentima $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$.

Stav 4.1 *Neka je $V \subset \mathbb{R}^m$ vektorski prostor.*

(i) Postoji baza za V.

(ii) Svake dve baze iz V imaju isti broj elemenata. Broj elemenata baze iz V je dimenzija vektorskog prostora V.

(iii) Neka je $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}$ baza u V i neka je $\boldsymbol{w_1}, \boldsymbol{w_2}, \ldots, \boldsymbol{w_n}$ drugi skup od n vektora iz V. Možemo napisati svaki vektor $\boldsymbol{w_j}$ kao linearnu kombinaciju vektora $\boldsymbol{v_i}$, tj.

$$\begin{aligned}
\boldsymbol{w_1} &= \alpha_{11}\boldsymbol{v_1} + \alpha_{12}\boldsymbol{v_2} + \cdots + \alpha_{1n}\boldsymbol{v_n},\\
\boldsymbol{w_2} &= \alpha_{21}\boldsymbol{v_1} + \alpha_{22}\boldsymbol{v_2} + \cdots + \alpha_{2n}\boldsymbol{v_n},\\
&\vdots \qquad\qquad\qquad \vdots\\
\boldsymbol{w_n} &= \alpha_{n1}\boldsymbol{v_1} + \alpha_{n2}\boldsymbol{v_2} + \cdots + \alpha_{nn}\boldsymbol{v_n},
\end{aligned}$$

Onda je $\boldsymbol{w_1}, \ldots, \boldsymbol{w_n}$ takođe baza iz V ako i samo ako je determinanta matrice različita od nule, tj.

$$\begin{vmatrix}
\alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n}\\
\alpha_{21} & a_{22} & \cdots & \alpha_{2n}\\
\vdots & \vdots & \ddots & \vdots\\
\alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn}
\end{vmatrix} \neq 0.$$

Definicija 4.2 *Neka su $\boldsymbol{v}, \boldsymbol{w} \in V \subset \mathbb{R}^m$. Ako napišemo $\boldsymbol{v}$ i $\boldsymbol{w}$ preko koordinata tada je*

$$\boldsymbol{v} = (x_1, x_2, \ldots, x_m) \quad i \quad \boldsymbol{w} = (y_1, y_2, \ldots, y_m).$$

Skalarni proizvod vektora $\boldsymbol{v}$ i $\boldsymbol{w}$ je

$$\boldsymbol{v} \cdot \boldsymbol{w} = x_1y_1 + x_2y_2 + \cdots + x_my_m.$$

Kažemo da su $\boldsymbol{v}$ i $\boldsymbol{w}$ ortogonalni ako je njihov skalarni proizvod $\boldsymbol{v} \cdot \boldsymbol{w} = 0$. Dužina ili norma vektora $\boldsymbol{v}$ je

$$\|\boldsymbol{v}\| = \sqrt{x_1^2 + x_2^2 + \cdots + x_m^2}.$$

Skalarni proizvod norme je dat formulom

$$\boldsymbol{v} \cdot \boldsymbol{v} = \|\boldsymbol{v}\|^2.$$

4.1 Pregled teorije rešetki

Prva opšta istraživanja rešetki počeli su poznati matematičari Žozef-Luj Lagranž [1] i Karl Fridrih Gaus [2], dok je istraživač Mikloš Ajtai [3] 1996. godine prvi put prikazao mogućnost primene rešetke u kriptografiji.

[1] *Joseph−Louis Lagrange* (1736-1813) bio je italijansko-francuski matematičar i astronom. Radio je na svim poljima analize i teorije brojeva, kao i na klasičnoj i nebeskoj mehanici.

[2] *Carl Friedrich Gauss* (1777-1855) bio je nemački matematičar koji je dao značajan doprinos u teoriji brojeva, analizi, diferencijalnoj geometriji itd. Smatra se jednim od najvećih matematičara u istoriji.

[3] *Miklós Ajtai* (1946) je mađarski programer i informatičar, danas živi i radi u SAD-u.

Definicija 4.3 *Neka je* $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n} \in \mathbb{R}^m$ *skup linearno nezavisnih vektora. Rešetka* L *generisana sa* $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}$ *je skup svih celobrojnih linearnih kombinacija vektora* $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}$,

$$L = \{a_1\boldsymbol{v_1} + a_2\boldsymbol{v_2} + \ldots + a_n\boldsymbol{v_n} : a_1, a_2, \ldots, a_n \in \mathbb{Z}\}.$$

Primetimo da je $m \geq n$. *Baza rešetke* L *je bilo koji skup linearno nezavisnih vektora koji generišu* L. *Svake dve baze rešetke* L *imaju isti broj elemenata. Dimenzija* L *je broj vektora u bazi rešetke* L.

Pretpostavimo da je $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}$ baza rešetke L i da je $\boldsymbol{w_1}, \boldsymbol{w_2}, \ldots, \boldsymbol{w_n} \in L$ drugi skup vektora iz L.
Slično kao i za vektorski prostor možemo svako $\boldsymbol{w_j}$ predstaviti kao linearnu kombinaciju baznih vektora:

$$\begin{aligned}
\boldsymbol{w_1} &= a_{11}\boldsymbol{v_1} + a_{12}\boldsymbol{v_2} + \cdots + a_{1n}\boldsymbol{v_n},\\
\boldsymbol{w_2} &= a_{21}\boldsymbol{v_1} + a_{22}\boldsymbol{v_2} + \cdots + a_{2n}\boldsymbol{v_n},\\
&\vdots \qquad\qquad\qquad\quad \vdots\\
\boldsymbol{w_n} &= a_{n1}\boldsymbol{v_1} + a_{n2}\boldsymbol{v_2} + \cdots + a_{nn}\boldsymbol{v_n},
\end{aligned}$$

s tim što su svi a_{ij} celi brojevi.

Ako pokušamo da izrazimo $\boldsymbol{v_i}$ preko $\boldsymbol{w_j}$, to će podrazumevati proces traženja inverzne matrice matrici

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}.$$

Ako želimo da su $\boldsymbol{v_i}$ celobrojne linearne kombinacije vektora $\boldsymbol{w_j}$ onda je potrebno da elementi matrice A^{-1} budu celi brojevi. Dakle

$$1 = \det(I) = \det\left(AA^{-1}\right) = \det(A)\det\left(A^{-1}\right),$$

gde su $\det(A)$ i $\det\left(A^{-1}\right)$ celi brojevi, pa mora da važi $\det(A) = \pm 1$. Obrnuto, ako je $\det(A) = \pm 1$, iz teorije matrica imamo da A^{-1} mora imati celobrojne elemente.

Stav 4.4 *Bilo koje dve baze rešetke* L *su povezane matricom, koja sadrži celobrojne koeficijente i determinantu koja je jednaka* ± 1.

Često je pogodno raditi sa rešetkama čiji vektori imaju celobrojne koordinate. Na primer, $\mathbb{Z}^n = \{(x_1, x_2, \ldots, x_n) : x_1, \ldots, x_n \in \mathbb{Z}\}$ je rešetka koja se sastoji od svih vektora sa celobrojnim koordinatama.

Definicija 4.5 *Integralna (ili celobrojna) rešetka je rešetka čiji svi vektori imaju celobrojne koordinate. Ekvivalentno, integralna rešetka je aditivna podgrupa* $\mathbb{Z}^m$ *Abelove grupe za neko* $m \geq 1$.

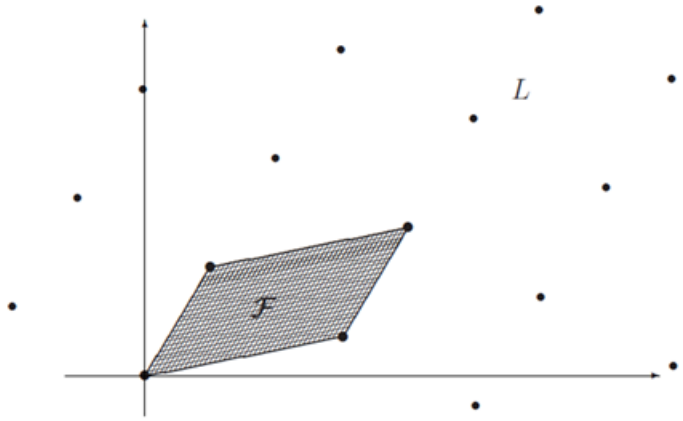
Definicija 4.6 *Podskup L prostora $\mathbb{R}^m$ je aditivna podgrupa ako je zatvoren u odnosu na sabiranje i oduzimanje. Naziva se diskretnom aditivnom podgrupom ako postoji pozitivna konstanta $\varepsilon > 0$ sa sledećim svojstvom: za svako $\boldsymbol{v} \in L$*

$$L \cap \{\boldsymbol{w} \in \mathbb{R}^m : \|\boldsymbol{v} - \boldsymbol{w}\| < \varepsilon\} = \{\boldsymbol{v}\}.$$

Odavde vidimo da za svaki vektor $\boldsymbol{v} \in L$, lopta oko $\boldsymbol{v}$ poluprečnika ε ne sadrži niti jedan drugi vektor iz rešetke osim $\boldsymbol{v}$.

Teorema 4.7 *Podskup prostora $\mathbb{R}^m$ je rešetka ako i samo ako je diskretna aditivna podgrupa.*

Često je korisno gledati na rešetku kao uređen raspored tačaka u $\mathbb{R}^m$, gde stavljamo tačku na vrh svakog vektora. Jedan primer rešetke u $\mathbb{R}^2$ je ilustrovan na slici 4.1 ispod.



Slika 4.1: Rešetka L i fundamentalni domen $\mathcal{F}$

Definicija 4.8 *Neka je L rešetka dimenzije n i neka je $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}$ baza u L. Fundamentalni domen (ili fundamentalni paralelopiped) za L koji odgovara ovoj bazi je skup $\mathcal{F}(\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}) = \{t_1\boldsymbol{v_1} + \ldots + t_n\boldsymbol{v_n} : 0 \leq t_i < 1\}$.*

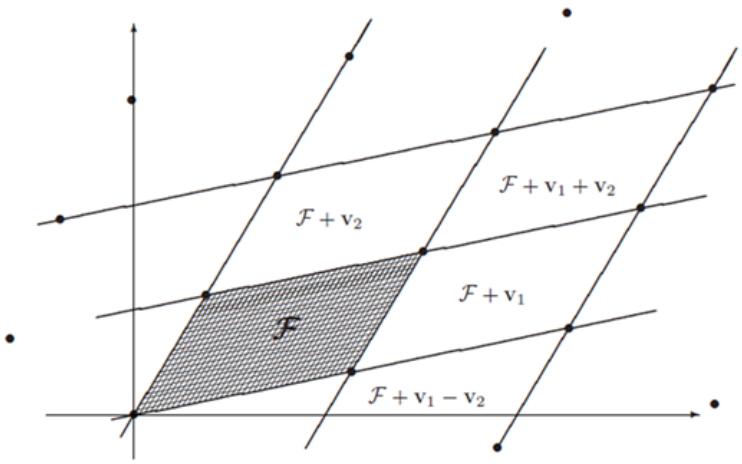
Stav 4.9 *Neka je $L \subset \mathbb{R}^n$ rešetka dimenzije n i neka je $\mathcal{F}$ fundamentalni domen za L. Tada se vektor $\boldsymbol{w} \in \mathbb{R}^n$ može zapisati u obliku*

$$\boldsymbol{w} = t + \boldsymbol{v} \quad \text{za jedinstveno } t \in \mathcal{F} \text{ i jedinstveno } \boldsymbol{v} \in L.$$

Ekvivalentno, unija transliranih fundamentalnih domena

$$\mathcal{F} + \boldsymbol{v} = \{t + \boldsymbol{v} : t \in \mathcal{F}\},$$

gde $\boldsymbol{v}$ prolazi rešetkom L pokriva celo $\mathbb{R}^n$ (videti sliku 4.2).



Slika 4.2: Translacija $\mathcal{F}$ vektorima $\boldsymbol{v}$ u rešetki L u $\mathbb{R}^n$

Dokaz. Neka je $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$ baza rešetke L koja daje fundamentalni domen $\mathcal{F}$. Onda su vektori $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$ linearno nezavisni u $\mathbb{R}^n$ i čine bazu u $\mathbb{R}^n$. To znači da bilo koji $\boldsymbol{w} \in \mathbb{R}^n$ može biti zapisan u obliku

$$\boldsymbol{w} = \alpha_1 \boldsymbol{v_1} + \alpha_2 \boldsymbol{v_2} + \cdots + \alpha_n \boldsymbol{v_n} \quad \text{za} \quad \alpha_1, \ldots, \alpha_n \in \mathbb{R}.$$

Za svako α_i imamo

$$\alpha_i = t_i + a_i,$$

gde je $0 \leq t_i < 1$ i $a_i \in \mathbb{Z}$. Tada je

$$\boldsymbol{w} = \overbrace{t_1 \boldsymbol{v_1} + t_2 \boldsymbol{v_2} + \cdots + t_n \boldsymbol{v_n}}^{\text{vektor } t \in \mathcal{F}} + \overbrace{a_1 \boldsymbol{v_1} + a_2 \boldsymbol{v_2} + \cdots + a_n \boldsymbol{v_n}}^{\text{vektor } v \in L}.$$

Ovo pokazuje da $\boldsymbol{w}$ može biti zapisan u željenoj formi.

Dalje, pretpostavimo da $\boldsymbol{w} = t + \boldsymbol{v} = t' + \boldsymbol{v'}$ ima dve reprezentacije kao suma vektora iz $\mathcal{F}$ i L. Onda je

$$\begin{aligned}&(t_1 + a_1)\boldsymbol{v_1} + (t_2 + a_2)\boldsymbol{v_2} + \cdots + (t_n + a_n)\boldsymbol{v_n} = \\ &= (t_1' + a_1')\boldsymbol{v_1'} + (t_2' + a_2')\boldsymbol{v_2'} + \cdots + (t_n' + a_n')\boldsymbol{v_n'}.\end{aligned}$$

Kako su $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$ linearno nezavisni, sledi da je

$$t_i + a_i = t_i' + a_i' \quad \text{za sve} \quad i = 1, 2, \ldots, n.$$

Stoga je

$$t_i - t_i' = a_i - a_i' \in \mathbb{Z}$$

ceo broj. Znamo da su t_i i t_i' veći ili jednaki 0 i strogo manji od 1, pa je jedini način da $t_i - t_i'$ bude ceo broj da $t_i = t_i'$. Dakle, kako je $t = t'$, imamo da je

$$\boldsymbol{v} = \boldsymbol{w} - t = \boldsymbol{w} - t' = \boldsymbol{v'}.$$

Ovim smo dokazali da su $t \in \mathcal{F}$ i $\boldsymbol{v} \in L$ jedinstveno određeni sa $\boldsymbol{w}$. ■

Ispostavlja se da svi fundamentalni domeni rešetke L imaju istu zapreminu. Ovo ćemo dokazati kasnije za rešetke dimenzija n u $\mathbb{R}^n$. Zapremina fundamentalnog domena je izuzetno važna invarijanta rešetke.

Nadalje, definišemo determinantu rešetke L.

Definicija 4.10 *Neka je L rešetka dimenzije n i neka je $\mathcal{F}$ fundamentalni domen za L. Tada n-dimenzionalnu zapreminu domena $\mathcal{F}$ nazivamo determinantom rešetke L. Obeležava se sa* $\det(L)$.

Vektore baze rešetke L možemo posmatrati kao stranice fundamentalnog domena $\mathcal{F}$. Tada je zapremina najveća ako su vektori međusobno ortogonalni. Sledeći stav nam daje gornje ograničenje za $\det(L)$.

Stav 4.11 *(Adamarova[4] nejednakost). Neka je L rešetka, a $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}$ bilo koja baza za L i neka je $\mathcal{F}$ fundamentalni domen za L. Tada važi*

$$\det L = V\big(\mathcal{F}\big) \leq \|\boldsymbol{v_1}\|\|\boldsymbol{v_2}\| \ldots \|\boldsymbol{v_n}\|.$$

Dokaz. Dokaz ćemo sprovesti koristeći QR dekompoziciju. Svaka matrica A može se predstaviti u obliku

$$A = QR,$$

gde je Q ortogonalna, a R gornja trougaona matrica (kolone matrice Q su takve da čine ortonormiranu bazu). Neka q_j označavaju kolone matrice Q, a_j kolone matrice A (za $j = 1, \ldots, n$) i neka su r_{ij} elementi matrice R.
Tada je

$$a_j = \sum_{i=1}^{j} r_{ij} q_i.$$

Odavde je

$$\|a_j\|^2 = \sum_{i=1}^{j} |r_{ij}|^2 \|q_j\|^2 \geq |r_{jj}|^2 \implies |r_{jj}| \leq \|a_j\|.$$

Konačno imamo da je

$$|\det(A)| = |\det(Q)||\det(R)| = 1 \cdot \left| \prod_{j=1}^{n} r_{jj} \right| \leq \prod_{j=1}^{n} \|a_j\|$$

što je i trebalo dokazati. ■

Sada definišemo Adamarovu srazmeru baze $\mathcal{B} = \{\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}\}$ sa vrednošću

$$\mathcal{H}(\mathcal{B}) = \left(\frac{\det L}{\|\boldsymbol{v_1}\|\|\boldsymbol{v_2}\| \ldots \|\boldsymbol{v_n}\|} \right)^{1/n}. \tag{4.2}$$

Tako je $0 < \mathcal{H}(\mathcal{B}) \leq 1$, pa što je vrednost bliža 1 to su vektori više ortogonalni u bazi.

[4] *Jacques Salomon Hadamard* (1865-1963), bio je francuski matematičar. Dao je značajan doprinos u teoriji parcijalnih diferencijalnih jednačina, diferencijalnoj geometriji, teoriji brojeva, funkcionalnoj analizi. Po njemu su nazvani Adamarov dinamički sistem, Adamarova matrica i Adamarova nejednakost.

Stav 4.12 *Neka je $L \subset \mathbb{R}^n$ rešetka dimenzije n i neka su vektori $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}$ baza za L, a $\mathcal{F}$ je fundamentalni domen generisan tom bazom. Koordinate i-tog vektora baze zapisujemo kao*

$$\boldsymbol{v_i} = (r_{i1}, \ldots, r_{in}),$$

i pomoću njih formiramo matricu

$$F = F(\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}) = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \ldots & r_{nn} \end{pmatrix}. \tag{4.3}$$

Tada je zapremina domena $\mathcal{F}$ data formulom

$$V\big(\mathcal{F}(\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n})\big) = \big|\det\big(F(\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n})\big)\big|. \tag{4.4}$$

Dokaz. Dokaz koristi višestruki račun. Možemo izračunati zapreminu $\mathcal{F}$ primenom integrala konstantne funkcije 1 na oblast $\mathcal{F}$.

$$V(\mathcal{F}) = \int\limits_{\mathcal{F}} dx_1\, dx_2 \ldots dx_n.$$

Fundamentalni domen $\mathcal{F}$ je skup opisan u Definiciji 4.8, tako da vršimo smenu promenljivih sa $x = (x_1, \ldots, x_n)$ na $t = (t_1, \ldots, t_n)$ u skladu sa formulom

$$(x_1, x_2, \ldots, x_n) = t_1\boldsymbol{v_1} + t_2\boldsymbol{v_2} + \cdots + t_n\boldsymbol{v_n}.$$

Na osnovu matrice $F = F(\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n})$ definisane u jednačini (4.3), smena promenljivih data je matričnom jednačinom $x = tF$. Jakobijeva matrica ove zamene promenljivih je F, a fundamentalni domen $\mathcal{F}$ je slika jedinične kocke $C_n = [0,1]^n$ pri preslikavanju F, tako da važi

$$\begin{aligned} \int\limits_{\mathcal{F}} dx_1\, dx_2 \ldots dx_n = \int\limits_{FC_n} dx_1\, dx_2 \ldots dx_n &= \int\limits_{C_n} |\det F| dt_1\, dt_2 \ldots dt_n \\ &= |\det F|\, V(C_n) = |\det F|. \end{aligned}$$

■

Posledica 4.13 *Neka je $L \subset \mathbb{R}^n$ rešetka dimenzije n. Tada svaki fundamentalni domen iz L ima istu zapreminu. Dakle,* $\det(L)$ *je nezavisna od odabira fundamentalnog domena.*

Dokaz. Neka su $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}$ i $\boldsymbol{w_1}, \boldsymbol{w_2}, \ldots, \boldsymbol{w_n}$ dva fundamentalna domena iz L i neka su $F(\boldsymbol{v_1}, \ldots, \boldsymbol{v_n})$ i $F(\boldsymbol{w_1}, \ldots, \boldsymbol{w_n})$ pridružene matrice (4.3) dobijene korišćenjem koordinata vektora kao vrsta matrica. Onda Stav 4.4 kaže da je

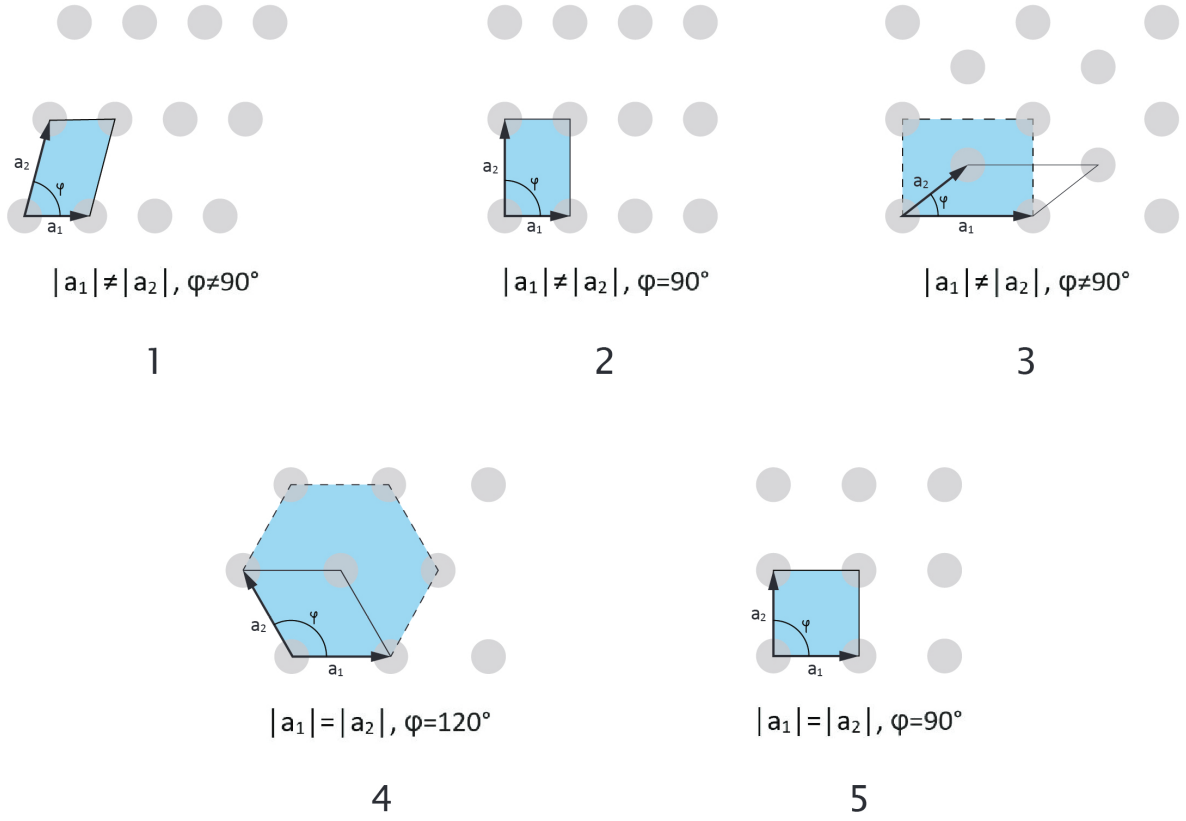
$$F(\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}) = AF(\boldsymbol{w_1}, \boldsymbol{w_2}, \ldots, \boldsymbol{w_n}) \tag{4.5}$$

za neku $n \times n$ matricu sa celobrojnim unosima i $\det(A) = \pm 1$. Ako primenimo Stav 4.12 dobijamo

$$
\begin{aligned}
&V\big(\mathcal{F}(\boldsymbol{v_1}, \ldots, \boldsymbol{v_n})\big) = \\
&\quad = \big|\det\big(F(\boldsymbol{v_1}, \ldots, \boldsymbol{v_n})\big)\big| \text{ iz Stava 4.12,} \\
&\quad = \big|\det\big(AF(\boldsymbol{w_1}, \ldots, \boldsymbol{w_n})\big)\big| \text{ iz izraza (4.5),} \\
&\quad = \big|\det(A)\big|\big|\det\big(F(\boldsymbol{w_1}, \ldots, \boldsymbol{w_n})\big)\big| \text{ kako je } \det(AB) = \det(A)\det(B), \\
&\quad = \big|\det\big(F(\boldsymbol{w_1}, \ldots, \boldsymbol{w_n})\big)\big| \text{ kako je } \det(A) = \pm 1, \\
&\quad = V\big(\mathcal{F}(\boldsymbol{w_1}, \ldots, \boldsymbol{w_n})\big) \text{ iz Stava 4.12.}
\end{aligned}
$$

■

Radi ilustracije sledećih pet primera rešetke se može definisati u euklidskoj ravni $\mathbb{R}^2$, sa bazom $(\boldsymbol{a_1}, \boldsymbol{a_2})$ (videti Sliku 4.3).



Slika 4.3: Pet osnovnih primera rešetke u euklidskoj ravni

4.2 Problem najkraćeg vektora i problem najbližeg vektora

Dva matematička problema koja se koriste u kriptosistemima na bazi rešetke, su problem najkraćeg vektora (engl. Shortest Vector Problem - SVP) i problem nalaženja najbližeg vektora (engl. Closest Vector Problem - CVP).

SVP problem se sastoji iz pronalaženja najkraćeg vektora u nekoj rešetki, za datu bazu rešetke. CVP problem zahteva da se, za datu bazu rešetke i neki vektor $\boldsymbol{v}$ koji nije deo rešetke, pronađe najkraći vektor koji pripada toj rešetki, a koji je najmanje udaljen od navedenog vektora $\boldsymbol{v}$.

Neke od varijanti SVP i CVP problema, koji se koriste u teoriji i praksi su:

- **Problem najkraće baze** (SBP): Nalazimo bazu $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$ koja je u nekom smislu najkraća za rešetku. Na primer, zahtevamo da

$$\max_{1 \leq i \leq n} \|\boldsymbol{v_i}\| \quad \text{ili} \quad \sum_{i=1}^{n} \|\boldsymbol{v_i}\|$$

  bude minimizirano. Postoje različite verzije SBP-a, u zavisnosti od načina merenja ,,veličine" baze.

- **Aproksimativni problem najkraćeg vektora** (apprSVP): Neka je $\psi(n)$ funkcija koja zavisi od n. U rešetki L dimenzije n, treba naći nenulti vektor čija je dužina najviše $\psi(n)$ puta veća od dužine najkraćeg vektora rešetke. Drugim rečima, ako je $\boldsymbol{v}_{shortest}$ najkraći nenulti vektor u L treba naći $\boldsymbol{v} \in L$ koji zadovoljava

$$\|\boldsymbol{v}\| \leq \psi(n)\|\boldsymbol{v}_{shortest}\|.$$

  Rešenje problema se menja izborom funkcije $\psi(n)$, kao što svaki izbor funkcije $\psi(n)$ daje drugačije appSVP. Kao konkretan primer, može se tražiti algoritam koji nalazi da je $\boldsymbol{v} \in L$ nenulti ako zadovoljava

$$\|\boldsymbol{v}\| \leq 3\sqrt{n}\|\boldsymbol{v}_{shortest}\| \quad \text{ili} \quad \|\boldsymbol{v}\| \leq 2^{n/2}\|\boldsymbol{v}_{shortest}\|.$$

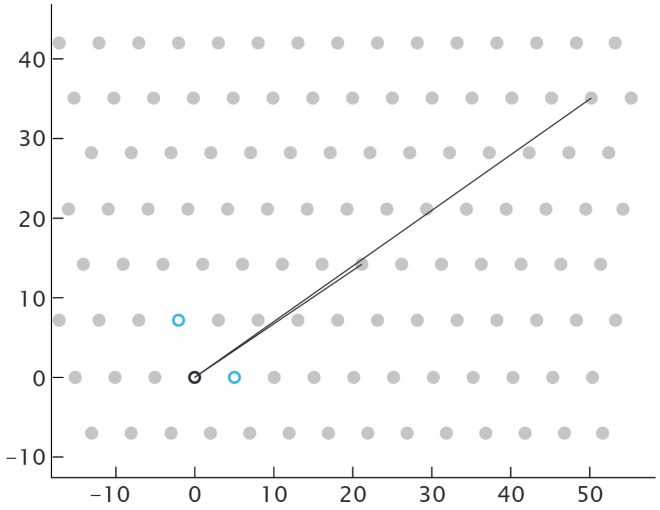
- **Aproksimativni problem najbližeg vektora** (apprCVP): Analogno appSVP, samo što ovde tražimo aproksimativno rešenje za CVP.

4.2.1 Problem najkraćeg vektora

Neka je data rešetka L. Treba naći nenula vektor $\boldsymbol{v}$ iz rešetke L, takav da je njegova euklidska norma $\|\boldsymbol{v}\|$ najmanja moguća.

Pošto za sada ne postoji efikasan algoritam koji će da reši SVP (CVP) u bilo kojoj izabranoj većoj dimenziji, uobičajeno je da se ovi problemi definišu kao aproksimacija početnog problema. Dati problem je naveden kao apprSVP.

Posmatrajmo sledeći primer rešetke koja je generisana vektorima $\boldsymbol{i}$=(50, 35) i $\boldsymbol{j}$=(21, 14) na $\mathbb{R}^2$ (videti sliku 4.4). Najkraći nenulti vektor je $\boldsymbol{a} = (5, 0)$. Sledeći najkraći vektor je $\boldsymbol{b} = (-2, 7)$.



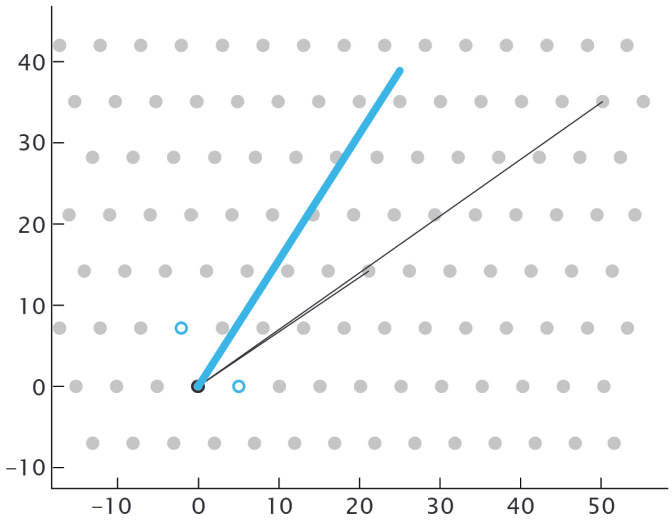
Slika 4.4: Primer SVP problema na rešetki L generisanoj na $\mathbb{R}^2$

4.2.2 Problem najbližeg vektora

Neka je data rešetka L. Za dati vektor $\boldsymbol{w}$ iz $\mathbb{R}^m$ koji ne pripada rešetki L treba naći vektor $\boldsymbol{v}$ koji pripada L i koji mu je najbliži, odnosno takav da je euklidska norma $\|\boldsymbol{w}-\boldsymbol{v}\|$ najmanja moguća.

Kao i za SVP, postoji takođe i aproksimacija CVP problema. Odgovarajući problem smo nazvali apprCVP.

Posmatraćemo primer sa rešetkom L (videti sliku 4.5) koja je generisana kao u primeru SVP problema i slučajni vektor $\boldsymbol{v}$ (deblja linija), koji ne pripada rešetki L. Potrebno je pronaći vektor koji pripada rešetki L, a koji je najbliži vektoru $\boldsymbol{v}$.



Slika 4.5: Primer CVP problema na rešetki L generisanoj na $\mathbb{R}^2$

5. Babai-ev algoritam

Ako rešetka $L \subset \mathbb{R}^n$ ima bazu $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$ koja sadrži vektore koji su u parovima ortogonalni, tj.

$$\boldsymbol{v_i} \cdot \boldsymbol{v_j} = 0, \text{ za svako } i \neq j,$$

problemi SVP i CVP se lako rešavaju. Dakle, za računanje SVP razmatramo dužinu bilo kog vektora u L, datu formulom

$$\|a_1\boldsymbol{v_1} + a_2\boldsymbol{v_2} + \ldots + a_n\boldsymbol{v_n}\|^2 = a_1^2\|\boldsymbol{v_1}\|^2 + a_2^2\|\boldsymbol{v_2}\|^2 + \ldots + a_n^2\|\boldsymbol{v_n}\|^2.$$

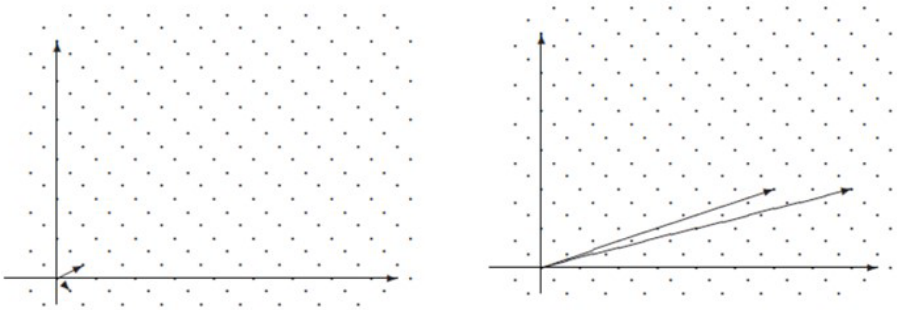
Kako su koeficijenti $a_1, \ldots, a_n \in \mathbb{Z}$, vidimo da su najkraći nenulti vektori u L zapravo najkraći vektori iz skupa $\{\pm\boldsymbol{v_1}, \ldots, \pm\boldsymbol{v_n}\}$. Slično, pretpostavimo da želimo da nađemo vektor u L koji je najbliži datom vektoru $\boldsymbol{w} \in \mathbb{R}^n$. Kako je $L \subset \mathbb{R}^n$ i L je dimenzije n, postoje koeficijenti $t_1, \ldots, t_n \in \mathbb{R}$ takvi da je

$$\boldsymbol{w} = t_1\boldsymbol{v_1} + t_2\boldsymbol{v_2} + \ldots + t_n\boldsymbol{v_n}.$$

Tako za vektor $\boldsymbol{v} = a_1\boldsymbol{v_1} + a_2\boldsymbol{v_2} + a_n\boldsymbol{v_n} \in L$ imamo:

$$\|\boldsymbol{v} - \boldsymbol{w}\|^2 = (a_1 - t_1)^2\|\boldsymbol{v_1}\|^2 + (a_2 - t_2)^2\|\boldsymbol{v_2}\|^2 + \ldots + (a_n - t_n)^2\|\boldsymbol{v_n}\|^2. \tag{5.1}$$

Koeficijenti a_i su celi brojevi, pa je jednakost (5.1) minimizirana ako za svako a_i uzmemo onaj celi broj koji je najbliži odgovarajućem t_i.



,,dobra baza" ,,loša" baza

Slika 5.1: Dve različite baze za jednu istu rešetku

Ovaj postupak neće dobro rešiti probleme SVP-a i CVP-a za one baze rešetke čiji vektori nisu ortogonalni. Na slici 5.1 su prikazane dve baze za istu rešetku. Prva baza je ,,dobra", u smislu da su vektori stvarno ortogonalni, a druga baza je ,,loša", jer je ugao između baznih vektora prilično mali.

Teorema 5.1 *(Babai-ev Algoritam najbližeg čvora). Neka je $L \subset \mathbb{R}^n$ rešetka sa bazom $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$ i neka je $\boldsymbol{w} \in \mathbb{R}^n$ proizvoljan vektor. Ako su vektori baze dovoljno*[1] *ortogonalni jedan prema drugom, problem CVP možemo rešiti na sledeći način:*

Pišemo $\boldsymbol{w} = t_1\boldsymbol{v_1} + t_2\boldsymbol{v_2} + \ldots + t_n\boldsymbol{v_n}$, gde su $t_1, \ldots, t_n \in \mathbb{R}$.
Postavimo $a_i = [t_i]$ za $i = 1, 2, \ldots, n$, gde je $[t_i]$ najbliži ceo broj broja t_i.
Rešenje problema je vektor $\boldsymbol{v} = a_1\boldsymbol{v_1} + a_2\boldsymbol{v_2} + \ldots + a_n\boldsymbol{v_n}$.

5.1 Primer 1

Neka je $L \subset \mathbb{R}^2$ rešetka sa datom bazom

$$\boldsymbol{v_1} = (137, 312) \quad \text{i} \quad \boldsymbol{v_2} = (215, -187).$$

Koristićemo Babai-ev algoritam (Teorema 5.1) da nađemo vektor u L koji je blizu vektoru

$$\boldsymbol{w} = (53172, 81743).$$

Prvi korak je da izrazimo $\boldsymbol{w}$ kao linearnu kombinaciju vektora $\boldsymbol{v_1}$ i $\boldsymbol{v_2}$ koristeći realne koordinate. Ovo radimo koristeći linearnu algebru. Treba da nađemo $t_1, t_2 \in \mathbb{R}$ tako da

$$\boldsymbol{w} = t_1\boldsymbol{v_1} + t_2\boldsymbol{v_2}.$$

Dobijamo dve linearne jednačine

$$53172 = 137t_1 + 215t_2 \quad \text{i} \quad 81743 = 312t_1 - 187t_2, \tag{5.2}$$

ili zapisano u obliku matrice

$$(53172, 81743) = (t_1, t_2)\begin{pmatrix} 137 & 312 \\ 215 & -187 \end{pmatrix}. \tag{5.3}$$

Lako se nalaze (t_1, t_2), bilo rešavanjem sistema jednačina (5.2) ili inverzijom matrice (5.3). Nalazimo da je $t_1 \approx 296.85$, a $t_2 \approx 58.15$. Babai-ev algoritam kaže da t_1 i t_2 zaokružimo najbližim celim brojem i onda rešimo

$$\boldsymbol{v} = [t_1]\boldsymbol{v_1} + [t_2]\boldsymbol{v_2} = 297(137, 312) + 58(215, -187) = (53159, 81818).$$

Tada je $\boldsymbol{v}$ u L i $\boldsymbol{v}$ treba da bude blizu $\boldsymbol{w}$. Nalazimo da je

$$\|\boldsymbol{v} - \boldsymbol{w}\| \approx 76.12,$$

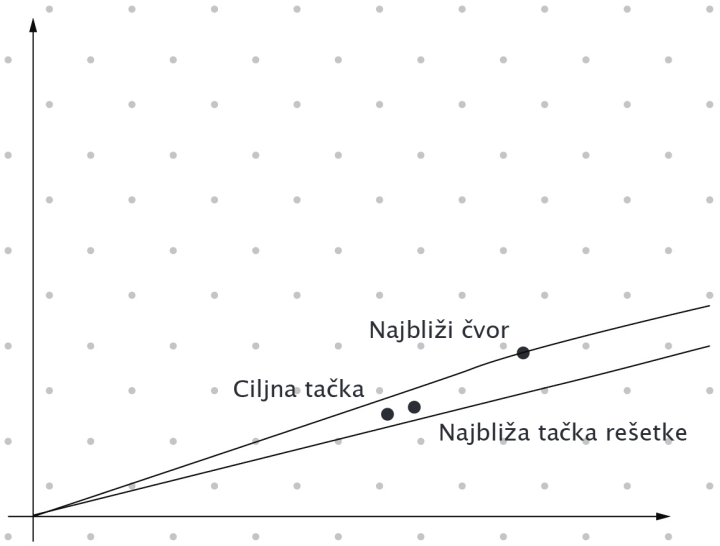
[1] Vektori baze su dovoljno ortogonalni ukoliko je Adamarova srazmera blizu jedinici.

što je zaista malo. Ovo se očekivalo, jer su vektori međusobno dovoljno ortogonalni u datoj bazi, što se vidi iz činjenice da je Adamarova srazmera

$$\mathcal{H}(\boldsymbol{v_1}, \boldsymbol{v_2}) = \left(\frac{\det(L)}{\|\boldsymbol{v_1}\|\|\boldsymbol{v_2}\|} \right)^{1/2} \approx \left(\frac{92699}{(340.75)(284.95)} \right)^{1/2} \approx 0.977$$

blizu 1.

Ako pokušamo da rešimo CVP koristeći ,,lošu" bazu, naići ćemo na problem kao što je prikazano na slici 5.2 ispod. Ciljna tačka koja nije u rešetki je zapravo prilično blizu tačke rešetke, ali je paralelogram toliko izdužen da je najbliži čvor ciljanoj tački prilično daleko. Važno je još zapaziti da sve postaje komplikovanije kako se dimenzija rešetke uvećava.



Slika 5.2: Babai-ev algoritam radi loše ako je baza ,,loša"

5.2 Primer 2

Probaćemo da rešimo isti najbliži vektorski problem u istoj rešetki, ali koristeći novu bazu

$$\boldsymbol{v_1'} = (1975, 438) = 5\boldsymbol{v_1} + 6\boldsymbol{v_2} \quad \text{i} \quad \boldsymbol{v_2'} = (7548, 1627) = 19\boldsymbol{v_1} + 23\boldsymbol{v_2}.$$

Sistem linearnih jednačina

$$(53172, 81743) = (t_1, t_2) \begin{pmatrix} 1975 & 438 \\ 7548 & 1627 \end{pmatrix} \tag{5.4}$$

ima rešenje $(t_1, t_2) \approx (5722.66, -1490.34)$, pa smo dobili da je

$$\boldsymbol{v'} = 5723\boldsymbol{v_1'} - 1490\boldsymbol{v_2'} = (56405, 82444).$$

Onda $\boldsymbol{v'} \in L$, ali $\boldsymbol{v'}$ nije naročito blizu $\boldsymbol{w}$, pa je

$$\|\boldsymbol{v'} - \boldsymbol{w}\| \approx 3308.12.$$

Neortogonalnost baze $\{\boldsymbol{v_1'}, \boldsymbol{v_2'}\}$ data je malom veličinom Adamarove srazmere

$$\mathcal{H}(\boldsymbol{v_1'}, \boldsymbol{v_2'}) = \left(\frac{\det(L)}{\|\boldsymbol{v_1'}\|\|\boldsymbol{v_2'}\|}\right)^{1/2} \left(\frac{92699}{(2022.99)(7721.36)}\right)^{1/2} \approx 0.077.$$

6. Kriptosistemi zasnovani na složenosti rešetke

Sredinom 90-tih su bili uvedeni neki kriptosistemi čiji su osnovni problemi bili SVP i/ili CVP u rešetki L dimenzije n. Najvažniji od njih su Ajtar-Dwork kriptosistem, GGH kriptosistem (Goldreich, Goldwasser i Halvei) i NTRU kriptosistem (Hofstajn [1], Pajfer [2], Silverman [3]).

Motivacija za uvođenje ovih kriptosistema je bila dvostruka. Prvo, svakako je od interesa imati kriptosisteme zasnovane na različitim teškim matematičkim problemima. Drugo, kriptosistemi zasnovani na rešetki su mnogo brži od faktorizacije ili problema diskretnog logaritma kao što su EL Gamal, RSA, ECC. Grubo govoreći, u cilju postizanja k bita sigurnosti enkripcija i dekripcija za El Gamal, RSA i ECC zahreva $\mathcal{O}(k^3)$ operacija, dok enkripcija i dekripcija za sisteme bazrane na rešetki zahteva $\mathcal{O}(k^2)$ operacija. Dalje, jednostavne operacije iz linearne algebre jednostavno je implementirati softverski i hardverski. Moramo napomenuti da analiza sigurnosti kriptosistema zasnovanih na teoriji brojeva i diskretnom logaritmu nije ni približno objašnjena, kao što je to slučaj sa sistemima zasnovanim na rešetki. Ipak jako je malo takvih sistema u poređenju sa kriptosistemima kao što je RSA.

6.1 GGH kriptosistem sa javnim ključem

GGH kriptosistem je jedan od najzapaženijih kriptosistema zasnovanih na složenosti rešetke. GGH, kao i drugi sistemi na bazi rešetke koristi problem najbližeg vektora (CVP). Osnovna ideja se sastoji u tome da je za bilo koju bazu rešetke jednostavno generisati vektor koji je blizu neke tačke koja pripada rešetki, na primer, uzimanjem neke tačke u rešetki i dodavanjem nekog malog vektora greške. S druge strane, da bi iz ovog novog vektora dobili prvobitni vektor koji pripada rešetki, potrebna je posebna baza.

Alisa počinje odabirom skupa linearno nezavisnih vektora $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n} \in \mathbb{Z}^n$ koji su dovoljno ortogonalni jedan u odnosu na drugi. Jedan način da se ovo uradi je da se fiksira parametar d i odaberu koordinate od $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$ nasumično između $-d$ i d. Alisa može da

[1] *Jeffrey Hoffstein* (1953) američki matematičar.
[2] *Jill Pipher* (1955) američka matematičarka.
[3] *Joseph Silverman* (1955) američki matematičar.

proveri da je njen izbor vektora dobar tako što računa Adamarovu srazmeru njene baze, uveravajući se da nije previše mala. Vektori $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$ su Alisin privatni ključ. Neka je V matrica dimenzije $n \times n$ takva da su vrste vektori $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$ i neka je L rešetka generisana ovim vektorima.

Alisa potom bira $n \times n$ matricu U sa celobrojnim koeficijentima i $\det(U) = \pm 1$. Jedan način da se kreira U je proizvod ogromnog broja nasumično odabranih elementarnih matrica. Ona onda računa

$$W = UV.$$

Vektori vrste $\boldsymbol{w_1}, \ldots, \boldsymbol{w_n}$ iz W su nova baza za L. Oni su Alisin javni ključ.

Kada Bob želi da pošalje Alisi poruku, on bira mali vektor $\boldsymbol{m}$ kao svoj otvoreni tekst, npr. $\boldsymbol{m}$ može biti binarni vektor. Bob takođe bira i mali nasumični vektor perturbacije $\boldsymbol{r}$ koji se ponaša kao privremeni ključ. Na primer, Bob može da odabere koordinate za $\boldsymbol{r}$ nasumično, izmedju $-\delta$ i δ, gde je δ javni fiksirani parametar. Bob onda računa vektor

$$\boldsymbol{e} = \boldsymbol{m}W + \boldsymbol{r} = \sum_{i=1}^{n} \boldsymbol{m}_i \boldsymbol{w}_i + \boldsymbol{r},$$

koji je njegov šifrovani tekst. Zapazimo da $\boldsymbol{e}$ nije tačka u rešetki, ali je blizu $\boldsymbol{m}W$ tačke rešetke, jer je $\boldsymbol{r}$ mali.

Dešifrovanje je jasno. Alisa koristi Babai-ev algoritam, kao što je opisano u prethodnom poglavlju, sa ,,dobrom" bazom $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$ da pronađe vektor u L koji je blizu $\boldsymbol{e}$. Pošto ona koristi dobru bazu i $\boldsymbol{r}$ je malo, vektor rešetke koji ona pronalazi je $\boldsymbol{m}W$. Onda ona množi sa W^{-1} da dođe do $\boldsymbol{m}$.

6.1.1 Primer

Ilustrujmo GGH kriptosistem 3-dimenzionalnim primerom. Za Alisinu privatnu dobru bazu uzimamo

$$\boldsymbol{v_1} = (-97, 19, 19),\ \boldsymbol{v_2} = (-36, 30, 86),\ \boldsymbol{v_3} = (-184, -64, 78).$$

Rešetka L generisana vektorima $\boldsymbol{v_1}, \boldsymbol{v_2}$ i $\boldsymbol{v_3}$ ima determinantu $\det(L) = 859516$ i Adamarova srazmera baze je

$$\mathcal{H}(\boldsymbol{v_1}, \boldsymbol{v_2}, \boldsymbol{v_3}) = \left(\det(L)/\|\boldsymbol{v_1}\|\|\boldsymbol{v_2}\|\|\boldsymbol{v_3}\|\right)^{1/3} \approx 0.74620.$$

Alisa množi svoju privatnu bazu matricom

$$U = \begin{pmatrix} 4327 & -15447 & 23454 \\ 3297 & -11770 & 17871 \\ 5464 & -19506 & 29617 \end{pmatrix},$$

koja ima determinantu $\det(U) = -1$, da bi stvorila javnu bazu

$$\begin{aligned} \boldsymbol{w_1} &= (-4179163, -1882253, 583183), \\ \boldsymbol{w_2} &= (-3184353, -1434201, 444361), \\ \boldsymbol{w_3} &= (-5277320, -2376852, 736426). \end{aligned}$$

Adamarova srazmera javnog ključa je veoma mala,

$$\mathcal{H}(\boldsymbol{w_1}, \boldsymbol{w_2}, \boldsymbol{w_3}) = \left(\det(L)/\|\boldsymbol{w_1}\|\|\boldsymbol{w_2}\|\|\boldsymbol{w_3}\|\right)^{1/3} \approx 0.0000208.$$

Bob odlučuje da pošalje Alisi prost tekst $\boldsymbol{m} = (86, -35, -32)$ koristeći nasumičnu perturbaciju $\boldsymbol{r} = (-4, -3, 2)$. Odgovarajući šifrovani tekst je

$$\begin{aligned}\boldsymbol{e} &= (86, -35, -32)\begin{pmatrix} -4179163 & -1882253 & 583183 \\ -3184353 & -1434201 & 444361 \\ -5277320 & -2376852 & 736426 \end{pmatrix} + (-4, -3, 2) \\ &= (-79081427, -35617462, 11035473).\end{aligned}$$

Alisa koristi Babai-ev algoritam za dekripciju. Ona prvo piše $\boldsymbol{e}$ kao linearnu kombinaciju svoje privatne baze sa realnim koeficijentom

$$\boldsymbol{e} = 81878.97\boldsymbol{v_1} - 292300\boldsymbol{v_2} + 443815.04\boldsymbol{v_3}.$$

Zaokružuje koeficijente najbližim celim brojem i računa vektor rešetke

$$\boldsymbol{v} = 81879\boldsymbol{v_1} - 292300\boldsymbol{v_2} + 443815\boldsymbol{v_3} = (-79081423, -35617459, 11035471)$$

koji je blizu $\boldsymbol{e}$. Alisa onda dolazi do $\boldsymbol{m}$ tako što izrazi $\boldsymbol{v}$ kao linearnu kombinaciju javne baze i iščita koeficijente,

$$\boldsymbol{v} = 86\boldsymbol{w_1} - 35\boldsymbol{w_2} - 32\boldsymbol{w_3}.$$

Sada pretpostavimo da Eva pokušava da dešifruje Bobovu poruku, ali ona zna samo javnu bazu $\boldsymbol{w_1}, \boldsymbol{w_2}, \boldsymbol{w_3}$. Ako primeni Babai-ev algoritam koristeći javnu bazu, ona pronalazi da je

$$\boldsymbol{e} \approx 75.76\boldsymbol{w_1} - 34.52\boldsymbol{w_2} - 24.18\boldsymbol{w_3}.$$

Kada zaokruži dobija vektor rešetke

$$\boldsymbol{v'} = 76\boldsymbol{w_1} - 35\boldsymbol{w_2} - 24\boldsymbol{w_3} = (-79508353, -35809745, 11095049)$$

što je na neki način blizu $\boldsymbol{e}$. Međutim, ovaj vektor rešetke daje netačan prost tekst $(76, -35, -24)$, a ne tačan prost tekst $\boldsymbol{m} = (86, -35, -32)$ koji je Bob poslao Alisi. Treba uporediti kako je Babai-ev algoritam dobro poslužio za različite baze. Onda pronalazimo da je

$$\|\boldsymbol{e} - \boldsymbol{v}\| \approx 5.3852 \quad \text{i} \quad \|\boldsymbol{e} - \boldsymbol{v'}\| \approx 472000.$$

Možemo zapaziti kako GGH kriptosistem nije siguran u dimenziji 3, pošto i kada koristimo brojeve koji su dovoljno veliki da naprave iscrpnu pretragu nepraktičnom, ima efikasnih algoritama[4] za pronalaženje dobre baze u manjoj dimenziji. U dimenziji 2, algoritam za pronalaženje dobre baze datira još od Gausa.

Alternativna verzija GGH preokreće uloge $\boldsymbol{m}$ i $\boldsymbol{r}$, tako da šifrovani tekst ima formu $\boldsymbol{e} = \boldsymbol{r}W + \boldsymbol{m}$. Alisa pronalazi $\boldsymbol{r}W$ računajući vektor rešetke najbliži $\boldsymbol{e}$ i onda otkriva prost tekst kao što je $\boldsymbol{m} = \boldsymbol{e} - \boldsymbol{r}W$.

[4]Efikasnost algoritma se meri potrošnjom vremena i prostora.

6.2 NTRU kriptosistem sa javnim ključem

Jedan od najzanimljivijih novijih kriptosistema, koji je još uvek predmet intenzivnog proučavanja je NTRU kriptosistem, koji su 1997. godine predložili Hofstajn, Pajfer i Silverman.

Sastoji se iz dva algoritma, NTRUEncrypt koji se koristi za šifrovanje i NTRUSign koji se koristi za digitalni potpis.

NTRUEncrypt je NTRU algoritam za šifrovanje koji se zasniva na problemu najkraćeg vektora (SVP) u rešetki. Operacije su zasnovane na objektima u količničkom polinomijalnom prstenu $R = \dfrac{\mathbb{Z}[x]}{(x^n - 1)}$ sa konvolutivnim množenjem, a svi polinomi u prstenu imaju celobrojne koeficijente stepena do $n - 1$

$$a = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1}.$$

NTRU je u stvari parametrizovana familija šifarskih sistema, a svaki sistem je definisan sa tri celobrojna parametra (n, p, q) koji predstavljaju maksimalni stepen $n - 1$ za sve polinome u skraćenom prstenu R, a zatim mali i veliki moduli p, q, respektivno, gde se podrazumeva da je n prost broj, q je uvek veće od p, q i p su uzajamno prosti brojevi ($\text{nzd}(p, q) = 1$), a četiri skupa polinoma L_f, L_g, L_m, L_r su: polinomijalni deo privatnog ključa, polinomi za generisanje javnog ključa, poruka i polinomi za zaklanjanje (sakrivanje) poruke, respektivno.

6.2.1 Primer

- Generisanje ključeva

Slanje tajne poruke od Alise do Boba zahteva generisanje privatnog i javnog ključa. Javni ključ naravno poseduju i Alisa i Bob, dok je privatni ključ poznat samo Bobu.

Da bi se generisao privatni-javni par ključeva, potrebna su dva polinoma f i g, najvećeg stepena $n-1$ i sa koeficijentima iz skupa $\{-1, 0, 1\}$. Polinom $f \in L_f$ mora da zadovolji dodatni zahtev da postoje inverz modulo q i inverz modulo p, što znači da je $f \cdot f_p = 1 \pmod p$ i $f \cdot f_q =$
$1 \pmod q$. Ako dati polinom f nije invertibilan potrebno je izabrati drugi polinom koji jeste. Oba polinoma f i f_p su Bobovi privatni ključevi. Javni ključ h je generisan sledećim izrazom:

$$h = p \cdot f_q \cdot g \pmod q.$$

Kao realni primer generisanja ključeva neka su izabrani sistemski parametri (n, p, q) sledeći: $n = 11, p = 3, q = 32$. Neka su navedeni sistemski parametri uvek svima poznati. Polinomi f i g su u ovom slučaju najviše reda 10 i oni mogu biti izabrani potpuno slučajno. U ovom primeru to su:

$$f = -1 + x + x^2 - x^4 + x^6 + x^9 - x^{10}$$
$$g = -1 + x^2 + x^3 + x^5 - x^8 - x^{10}.$$

Korišćenjem Euklidovog algoritam izračunate su inverzne vrednosti f mod p i f mod q:

$f_p = 1 + 2x + 12x^3 + 2x^4 + x^5 + 2x^7 + x^8 + 2x^9 \pmod 3$
$f_q = 5 + 9x + 6x^2 + 16x^3 + 4x^4 + 15x^5 + 16x^6 + 22x^7 + 20x^8 + 18x^9 + 30x^{10} \pmod{32}$.

Na osnovu dobijenog inverza polinoma f_q i drugog polinoma g dobije se javni ključ h:

$$h = p \cdot f_q \cdot g \pmod{32} = 8 + 25x + 22x^2 + \ldots + 19x^9 + 16x^{10} \pmod{32}.$$

- **Šifrovanje**

Alisa šalje tajnu poruku Bobu u obliku polinoma m sa koeficijentima $\{-1, 0, 1\}$. Ovaj polinom može da se reprezentuje u binarnom ili ternarnom obliku. Potom Alisa bira slučajan polinom r sa malim koeficijentima, koji ne moraju biti ograničeni na skup $\{-1, 0, 1\}$, koji se koristi da poruku učini nerazumljivom.
Uz pomoć Bobovog javnog ključa h, izračunata je poruka e

$$e = r \cdot h + m \pmod q.$$

Neka je tajna poruka koju Alisa šalje u obliku sledećeg polinoma m:

$$m = -1 + x^3 - x^4 + x^5 - x^8 + x^9 + x^{10}.$$

Neka je polinom r koji će da učini poruku nečitljivom

$$r = -1 + x^2 + x^3 + x^4 - x^5 - x^7.$$

Šifrovana poruka e koju Alisa šalje Bobu u tom slučaju je:

$$e = r \cdot h + m \pmod{32} =$$

$$= 14 + 11x + 26x^2 + 24x^3 + 14x^4 + 16x^5 + 30x^6 + 7x^7 + 25x^8 + 6x^9 + 19x^{10} \pmod{32}.$$

- **Dešifrovanje**

Na osnovu polinoma r može se izračunati poruka m, pa prema tome Alisa mora da održava polinom r tajnim. Uz sve poznate parametre Bob poseduje i svoj privatni ključ. Da bi dešifrovao poruku m, Bob prvo množi šifrovanu poruku e i deo svog privatnog ključa f.

$$a = f \cdot e \pmod q.$$

Na osnovu primera dobija se da je

$$a = f \cdot e \pmod{32} =$$
$$= 3 - 7x - 10x^2 - 11x^3 + 10x^4 + 7x^5 + 6x^6 + 7x^7 + 5x^8 - 3x^9 - 7x^{10} \pmod{32}.$$

Sledeći korak podrazumeva izračunavanje $a \bmod p$.

$$b = a \pmod p = f \cdot m \pmod p, \text{ zato što je } p \cdot r \cdot g \pmod p = 0.$$

Na osnovu primera dobija se

$$b = a \pmod 3 = -x - x^2 + x^3 + x^4 + x^5 + x^7 - x^8 - x^{10} \pmod 3.$$

Znajući vrednost b, Bob može da iskoristi drugi deo svog privatnog ključa f_p kako bi množenjem b i f_p dobio poruku.

$$c = f_p \cdot b = f_p \cdot f \cdot m \pmod p,$$

što znači da je $c = m \pmod p$ zbog uslova $f_p \cdot f = 1 \pmod p$ za f_p.
Na osnovu primera dobija se

$$\begin{gathered} c = m \pmod 3 = \\ = -1 + x^3 - x^4 + x^5 - x^8 + x^9 + x^{10}, \end{gathered}$$

što je zaista poruka koju je Alisa poslala Bobu u gornjem primeru.

- **Sigurnost**

Od pojavljivanja NTRU šifarskog sistema primećeno je nekoliko značajnih napada. Većina napada se fokusira na nalaženje tajnog ključa f umesto dešifrovanja poruke. Ako je poznato da f ima veoma mali broj nenula koeficijenata, napadač može da primeni napad grubom silom tako što će pokušati da proba sve moguće vrednosti f.

Moguće je primeniti napad čovek-u-sredini [5] koji je napredniji od napada grubom silom, jer je moguće da skrati vreme pretraživanja proporcionalno kvadratnom korenu. Ovaj napad se zasniva na činjenici da je

$$f \cdot h = g \ (\bmod p).$$

[5] MITM (Man in The Middle) napad funkcioniše tako što kreira vezu između napadnutih mašina i prosleđuje poruke između njih. Žrtve veruju da zaista komuniciraju jedna sa drugom, dok zapravo njihova komunikacija teče preko mašine koja izvodi napad. Rezultat ovakvog napada nije samo prisluškivanje poverljivih podataka, već i podmetanje i upravljanje podacima radi sticanja još veće kontrole nad žrtvama napada.

7. Zaključak

Kriptografija zasnovana na rešetkama nudi niz prednosti u odnosu na konvencionalne šifre. Neke od njih su sledeće:

- Poboljšana bezbednost,

- Brže vreme računanja,

- Manja potrošnja energije,

- Fleksibilnost i jednostavnost implementacije.

Ovaj rad ima za cilj da se prikažu osnove kriptosistema javnog ključa, a da se zatim prikažu osnovni kriptosistemi zasnovani na rešetkama. Čitalac se upoznaje sa teorijom rešetki koja je neophodna za dalje konstrukcije i susreće se sa dva računska problema u rešetkama: nalaženje najkraćeg nenula vektora u rešetki i nalaženje vektora rešetke koji je najbliži datom nenula vektoru rešetke.
Opisana su dva najpoznatija post-kvantna [1] šifarska sistema koja se zasnivaju na problemima rešetke: GGH i NTRU.

Očekuje se da će i drugi, novi, šifarski sistemi koji se zasnivaju na SVP i CVP problemima na rešetki, biti objavljeni u budućnosti, a veliki broj istraživača se bavi ovim poljem matematike.

[1] Post-kvantna kriptografija, takođe poznata kao kvantna enkripcija je razvoj kriptografskih sistema (post-kvantnih sistema) za klasične računare koji mogu sprečiti napade koje pokreću kvantni računari.

Literatura

[1] Jeffrey Hoffstein, Jill Pipher, Joshep H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, Science & Business Media, LLC, 2008.

[2] Bernstein, Daniel J., Johannes Buchmann, and Erik Dahmen, eds. *Post-quantum cryptography*, Springer, Science & Business Media, 2009.

[3] M. Živković, *Kriptografija*, Matematički fakultet, Beograd, 2000.

[4] Slaven Ijačić, *Primena kvantne mehanike u kriptografiji, kvantno računarstvo i postkvantni sistemi*, Univerzitet Singidunum, Beograd, 2014.

[5] Paeng, Seong-Hun, Bae Eun Jung, Kil-Chan Ha, *A lattice based public key cryptosystem using polynomial representations*, Springer Berlin Heidelberg, 2003.