Rešetke i kriptografija

Klarić, Matija

Master's thesis / Diplomski rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, School of Applied Mathematics and Informatics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet primijenjene matematike i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:365352

Sveučilište J.J. Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike
Sveučilišni diplomski studij matematike
smjer: Financijska matematika i statistika

Matija Klarić

Rešetke i kriptografija

Diplomski rad

Osijek, 2023.

Sveučilište J.J. Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike
Sveučilišni diplomski studij matematike
smjer: Financijska matematika i statistika

Matija Klarić

Rešetke i kriptografija

Diplomski rad

Mentor: prof. dr. sc. Ivan Matić

Osijek, 2023.

Sadržaj

Uvod **i**

1 Kongruencijski kriptosustav s javnim ključem **1**

2 Problemi suma podskupova i kritposustavi naprtnjače **5**

3 Kratak pregled vektorskih prostora **13**

4 Rešetke: Osnovne definicije i svojstva **17**

5 Kratki vektori u rešetkama **25**

5.1 Problem najkraćeg i problem najbližeg vektora 25

5.2 Hermiteov teorem i teorem Minkowskog 27

6 Babajev algoritam i rješavanje apprCVP pomoću "dobre" baze **31**

7 GGH kriptosustav s javnim ključem **36**

Literatura **40**

Sažetak **41**

Summary **42**

Životopis **43**

Uvod

Sigurnost većine kriptosustava s javnim ključem bazira se, izravno ili neizravno, na problemu faktorizacije velikih brojeva ili pak na težini pronalaska diskretnih logaritama u konačnim grupama. U ovom radu proučavat ćemo novi tip teškog problema koji se javlja u teoriji rešetki, a može se koristiti kao baza za kriptosustav s javnim ključem. Nadalje, vidjet ćemo da teorija rešetki u kriptografiji ima i dodatnih primjena.

Podsjetimo se da je vektorski prostor V nad poljem realnih brojeva $\mathbb{R}$ skup vektora u kojem dva vektora možemo zbrojiti, a vektor možemo pomnožiti realnim brojem. Rešetka je nešto slično vektorskom prostoru. Razlika je ta da smo u rešetci kod spomenutog množenja ograničeni samo na množenje s cijelim brojevima. Ova naizgled mala restrikcija dovodi do mnogih zanimljivih i delikatnih pitanja. S obzirom da se ova tematika može činiti nametljivom u smislu neuobičajenosti u kriptografiji, započet ćemo s dva motivacijska primjera u kojima nećemo spominjati rešetke, no one će se kriti u pozadini čekajući da budu iskorištene u kriptoanalizi. Nadalje ćemo dati kratak pregled teorije vektorskih prostora te nakon toga formalno uvesti rešetke.

1 Kongruencijski kriptosustav s javnim ključem

U ovom poglavlju opisat ćemo jedan pojednostavljen model stvarnog kriptosustava s javnim ključem. Ovakva verzija modela imat će neočekivanu povezanost s rešetkama dimenzije 2, a samim time i visoku ranjivost, jer je dimenzija tako mala. Kakogod, ovakav model instruktivan je kao primjer da se rešetke pojavljuju u kriptoanalizi čak i kad teški problem koji je u pozadini naizgled s njima nema nikakve veze. Nadalje, model se može koristiti kao uvod u NTRU kriptosustav s javnim ključem najmanje dimenzije.

Ana započinje odabirom velikog prirodnog broja q, koji je javni parametar, te još dva tajna prirodna broja f i g koji zadovoljavaju sljedeća svojstva:

$$f < \sqrt{q/2}, \qquad \sqrt{q/4} < g < \sqrt{q/2} \qquad \text{i} \qquad (f, q) = 1.$$

Zatim, Ana računa vrijednost

$$h \equiv f^{-1} g \pmod{q}, \qquad \text{gdje je} \qquad 0 < h < q.$$

Uočimo kako su f i g mali u odnosu na q, jer su $\mathcal{O}(\sqrt{q})$, dok je vrijednost h generalno $\mathcal{O}(q)$, što je znatno veće. Anin tajni ključ je par manjih prirodnih brojeva f i g, dok je njen javni ključ veći prirodni broj h.

Kako bi poslao poruku, Ivan odabire otvoreni tekst m te na slučajan način bira prirodan broj r (koji ćemo zvati kratkotrajni ključ) tako da su zadovoljene nejednakosti

$$0 < m < \sqrt{q/4} \qquad \text{i} \qquad 0 < r < \sqrt{q/2}.$$

Ivan zatim računa šifrat na način

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

i šalje ga Ani.

Ana dešifrira poruku tako da prvo računa

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

pa zatim

$$b \equiv f^{-1} a \pmod{g}, \qquad \text{gdje je} \qquad 0 < b < g. \tag{1}$$

Uočimo da je f^{-1} u (1) inverz od f modulo g.

Uvjerimo se prvo da je $b = m$, čime ćemo pokazati da je Ana otkrila Ivanov otvoreni tekst. Prvo uočimo da vrijednost a zadovoljava sljedeće:

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

Ograničenja na veličinu brojeva f, g, r, m povlače da je broj $rg + fm$ mali, odnosno

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

Stoga, kad Ana računa $a \equiv fe \pmod{q}$, uz $0 < a < q$, ona dobiva točnu vrijednost

$$a = rg + fm. \tag{2}$$

Ovo je ključno: formula (2) nije samo kongruencija modulo q nego jednakost cijelih brojeva.

Naposlijetku, Ana računa

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

gdje je $0 < b < g$. S obzirom da je $m < \sqrt{q/4} < g$, slijedi da je $b = m$.

Kongruencijski kriptosustav sažet je u Tablici 1 ([3, Table 6.1]).

Primjer 1. ([3, Example 6.1]) Ana odabire

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

Ovdje su $f \approx 0.66\sqrt{q}$ i $g \approx 0.56\sqrt{q}$ dozvoljene vrijednosti. Nakon toga, Ana računa

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

Anin javni ključ je par $(q, h) = (122430513841, 39245579300)$.

Ivan odlučuje Ani poslati otvoreni tekst $m = 123456$ koristeći slučajno odabranu vrijednost $r = 101010$. Koristi Anin javni ključ kako bi izračunao šifrat

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

koji zatim šalje Ani.

Kako bi dešifrirala e, Ana prvo koristi svoju tajnu vrijednost f za računanje

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

Ana	Ivan
Kreiranje ključa	
Odabire veliki prirodni broj q te tajne prirodne brojeve f i g takve da je $f < \sqrt{q/2}, \sqrt{q/4} < g < \sqrt{q/2}, (f,q) = 1.$ Računa $h \equiv f^{-1}g \pmod{q}$ te objavljuje javni ključ (q,h).	
Enkripcija	
	Odabire otvoreni tekst $m < \sqrt{q/2}$. Pomoću Aninog otvorenog ključa (q,h) računa $e \equiv rh + m \pmod{q}.$ Šalje šifrat e Ani.
Dekripcija	
Računa $a \equiv fe \pmod{e}, 0 < a < q$. Računa $b \equiv f^{-1}a \pmod{g}, 0 < b < g$. Dobiveni b je otvoreni tekst m.	

Tablica 1: Kongruencijski kriptosustav s javnim ključem

Uočimo da je $a = 48314309316 < 122430513841 = q$. Sljedeće, Ana koristi vrijednost $f^{-1} \equiv 193495 \pmod{g}$ kako bi izračunala

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

što je upravo Ivanov otvoreni tekst m.

Zapitajmo se sada kako bi treća osoba (nazovimo ju Marija) mogla napasti ovaj sustav. Mogla bi izvršiti pretragu primjenom grube sile (brute-force) kroz sve moguće tajne ključeve ili kroz sve moguće otvorene tekstove, ali bi to zahtijevalo $\mathcal{O}(q)$ operacija. Promotrimo detaljnije Marijin zadatak ukoliko pokuša pronaći tajni ključ (f,g) pomoću poznatog javnog ključa (q,h). Nije teško uvidjeti da, ukoliko Marija pronađe bilo koji par pozitivnih cijelih brojeva F i G koji zadovoljavaju

$$Fh \equiv G \pmod{q} \qquad \text{i} \qquad F = \mathcal{O}(\sqrt{q}) \qquad \text{i} \qquad G = \mathcal{O}(\sqrt{q}), \tag{3}$$

onda će (F,G) vjerojatno poslužiti kao dekripcijski ključ.

Zapišemo li kongruenciju (3) u obliku $Fh = G + qR$, reformulirali smo Marijin zadatak kao traženje para relativno malih cijelih brojeva (F,G) sa svojstvom

$$F(1,h) - R(0,q) = (F,G).$$

U ovoj jednakosti, F i R su nepoznati cijeli brojevi, $(1, h)$ i $(0, q)$ su poznati vektori, a (F, G) je nepoznati mali vektor.

Marija stoga zna vektore $v_1 = (1, h)$ i $v_2 = (0, q)$ koji oba imaju duljinu $\mathcal{O}(q)$. Želi pronaći linearnu kombinaciju $w = a_1 v_1 + a_2 v_2$ takvu da vektor w ima duljinu $\mathcal{O}(\sqrt{q})$, imajući na umu da koeficijenti a_1 i a_2 moraju biti cjelobrojni. Dakle, Marija treba pronaći kratak nenul vektor u skupu vektora

$$L = \{a_1 v_1 + a_2 v_2 \quad : \quad a_1, a_2 \in \mathbb{Z}\}.$$

Navedeni skup L primjer je dvodimenzionalne rešetke. Lako je uočiti da podsjeća na dvodimenzionalni vektorski prostor s bazom $\{v_1, v_2\}$, no dozvoljene su samo cjelobrojne linearne kombinacije baznih vektora. Nažalost za Ivana i Anu, a zahvaljujući Gaussu, postoji vrlo brza i učinkovita metoda za pronalazak kratkih vektora u dvodimenzionalnim rešetkama.

2 Problemi suma podskupova i kritposustavi naprtnjače

Prvi pokušaj baziranja kriptosustava na $\mathcal{NP}$-potpunom problemu proveli su Merkle i Hellman krajem 70-ih godina prošlog stoljeća. Koristili su verziju matematičkog problema kojeg ćemo u nastavku opisati, a koji generalizira klasični problem naprtnjače.

Pretpostavimo da je zadana lista prirodnih brojeva $(M_1, M_2, \ldots, M_n)$ te prirodni broj S. Treba pronaći podskup elemenata zadane liste čija je suma S, uz pretpostavku da postoji barem jedan takav.

Primjer 2. ([3, Example 6.2]) Neka je $M = (2, 3, 4, 9, 14, 23)$ i $S = 27$. Isprobavanjem dobivamo podskup $\{4, 9, 14\}$ čija je suma 27 i nije teško provjeriti da je to jedini podskup zadanog skupa s tom sumom. Slično, uzmemo li $S = 29$, tada podskup $\{2, 4, 23\}$ ima željenu sumu. Međutim, u ovom slučaju postoji i drugo rješenje, jer je suma podskupa $\{2, 4, 9, 14\}$ također 29.

Evo još jednog načina opisivanja problema suma podskupova. Neka je lista

$$M = (M_1, M_2, \ldots, M_n)$$

prirodnih brojeva javno poznata. Ivan odabire vektor $x = (x_1, x_2, \ldots, x_n)$ kao tajni binarni vektor, tj. svaki x_i je ili 0 ili 1. Zatim računa sumu

$$S = \sum_{i=1}^{n} x_i M_i$$

i šalje broj S Ani. Ana treba pronaći ili originalni vektor x ili neki drugi binarni vektor koji će dati istu sumu. Uočimo da vektor x govori Ani koji M_i uključiti u sumu S, s obzirom da je M_i u sumi S ako i samo ako je $x_i = 1$. Stoga je određivanje binarnog vektora x ekvivalentno određivanju pripadnog podskupa od M.

Jasno je da Ana može pronaći x provjerom svih 2^n binarnih vektora duljine n. Jednostavan kolizijski algoritam pomaže Ani prepoloviti eksponent n.

Propozicija 3. ([3, Proposition 6.3.]) *Neka je $M = (M_1, M_2, \ldots, M_n)$ te (M, S) zadani problem sume podskupa. Za sve skupove prirodnih brojeva I i J koji zadovoljavaju*

$$I \subset \{i : 1 \leq i \leq \frac{n}{2}\} \qquad i \qquad J \subset \{j : \frac{n}{2} < j \leq n\}$$

računamo i konstruiramo liste vrijednosti

$$A_I = \sum_{i \in I} M_i \qquad \text{i} \qquad B_J = S - \sum_{j \in J} M_j.$$

Tada dobivene liste uključuju par skupova $I_0 = J_0$ koji zadovoljavaju $A_{I_0} = B_{J_0}$ i daju rješenje problema sume podskupa,

$$S = \sum_{i \in I_0} M_i + \sum_{j \in J_0} M_j.$$

Broj elemenata pojedine liste je najviše $2^{n/2}$, pa je vrijeme izvršavanja algoritma $\mathcal{O}(2^{n/n+\epsilon})$, gdje je ϵ neka mala vrijednost koja ovisi o sortiranju i uspoređivanju lista.

Dokaz. Dovoljno je uočiti sljedeće: ako je x binarni vektor koji daje rješenje zadanog problema sume podskupa, tada rješenje možemo pisati u obliku

$$\sum_{1 \le i \le \frac{1}{2}n} x_i M_i = S - \sum_{\frac{1}{2}n < i \le n} x_i M_i.$$

Broj podskupova I i J je $\mathcal{O}(2^{n/2})$ pa su to podskupovi skupova reda veličine $n/2$. □

Ako je n velik, tada je općenito teško riješiti slučajno zadan problem sume podskupa. Pretpostavimo, međutim, da Ana posjeduje tajno znanje ili neku informaciju o M uz koju može tvrditi da je rješenje x jedinstveno i koja joj omogućuje da ga lako nađe. Tada Ana može koristiti problem sume podskupa kao kriptosustav s javnim ključem. Ivanov otvoreni tekst je vektor x, njegova šifrana poruka je suma $S = \sum x_i M_i$ i samo Ana može lako povratiti x poznavanjem S.

Zanima nas kakvim se trikom može poslužiti Ana kako bi osigurala da rješenje zadanog problema sume podskupa može pronaći ona i nitko više. Jedna mogućnost je koristiti problem koji je vrlo lako riješiti, ali na neki način zamaskirati to lagano rješenje od drugih.

Definicija. ([3, Poglavlje 6]) *Superrastući niz* cijelih brojeva je niz prirodnih brojeva $r = (r_1, r_2, \ldots, r_n)$ sa svojstvom

$$r_{i+1} \ge 2r_i \qquad \text{za sve} \qquad 1 \le i \le n-1.$$

Sljedeća ocjena objašnjava naziv takvih nizova.

Lema 4. ([3, Lemma 6.4.]) *Neka je $r = (r_1, r_2, \ldots, r_n)$ superrastući niz. Tada je*

$$r_k > r_{k-1} + \cdots + r_2 + r_1 \qquad \textit{za sve} \qquad 2 \le k \le n.$$

Dokaz. Provodimo dokaz indukcijom po k. Za $k = 2$ imamo $r_2 \ge 2r_1 > r_1$, što je baza indukcije. Sada pretpostavimo da je tvrdnja točna za neki $2 \le k < n$. Koristeći prvo činjenicu da je niz superrastući, a zatim i pretpostavku indukcije, dobivamo da je

$$r_{k+1} \geq 2r_k = r_k + r_k > r_k + (r_{k-1} + \cdots + r_2 + r_1).$$

Time je pokazano da tvrdnja vrijedi i za $k+1$. $\square$

Problem sume podskupa u kojem cijeli brojevi u M čine superrastući niz je vrlo lagan za riješiti.

Propozicija 5. ([3, Proposition 6.5.]) *Neka je (M, S) problem sume podskupa u kojem prirodni brojevi u M čine superrastući niz. Ukoliko rješenje x postoji, jedinstveno je i može se odrediti sljedećim algoritmom:*

Za i od n do 1 Ako je $S \geq M_i$, postavi $x_i = 1$ i oduzmi M_i od S. U suprotnom postavi $x_i = 0$.

Dokaz. Pretpostavka da je M superrastući niz znači da je $M_{i+1} \geq 2M_i$. S obzirom da pretpostavljamo da rješenje postoji, označimo stvarno rješenje s y kako bismo ga razlikovali od rješenja x dobivenog algoritmom. Dakle, pretpostavljamo da je $y \cdot M = S$ i trebamo pokazati da je $x = y$.

Dokazujemo indukcijom nadolje da je $x_k = y_k$ za sve $1 \leq k \leq n$. Induktivna pretpostavka je da je $x_i = y_i$ za sve $k < i \leq n$ i trebamo pokazati da je $x_k = y_k$. Uočimo da dopuštamo $k = n$. U tom slučaju je induktivna pretpostavka očito istinita. Pretpostavka znači da smo pri izvođenju algoritma od $i = n$ nadolje prema $i = k+1$ u svakom koraku imali $x_i = y_i$. Stoga se prije izvođenja petlje za $i = k$ vrijednost od S reducirala na

$$S_k = S - \sum_{i=k+1}^{n} x_i M_i = \sum_{i=1}^{n} y_i M_i - \sum_{i=k+1}^{n} x_i M_i = \sum_{i=1}^{k} y_i M_i.$$

Promotrimo sada što se dogodi pri izvođenju iteracije za $i = k$. Dvije su mogućnosti:

$$\begin{aligned} &(1) \quad y_k = 1 \Longrightarrow S_k \geq M_k && \Longrightarrow x_k = 1, \quad \checkmark \\ &(2) \quad y_k = 0 \Longrightarrow S_k \leq M_{k-1} + \cdots + M_1 < M_k && \Longrightarrow x_k = 0. \quad \checkmark \end{aligned}$$

U slučaju (2) smo pomoću Leme 4 zaključili da je $M_{k+1} + \cdots + M_1$ strogo manje od M_k. U oba slučaja, dakle, dobivamo da je $x_k = y_k$, čime je dokazano da je $x = y$. Nadalje, dokazana je i jedinstvenost, jer smo pokazali da se svako rješenje podudara s outputom algoritma, koji vraća jedinstveni vektor x za bilo koji zadani input S. $\square$

Primjer 6. ([3, Example 6.6.]) Niz $M = (3, 11, 24, 50, 115)$ je superrastući. U početku uzmimo $S = 142$ kao sumu elemenata u M slijedeći dani algoritam. Kako je $S \geq 115$, postavljamo $x_5 = 1$ i zamjenjujemo S sa $S - 115 = 27$. Zatim je $27 < 50$, pa postavljamo $x_4 = 0$. Imamo $27 \geq 24$ pa postavljamo $x_3 = 1$ i S postaje $27 - 24 = 3$. Nadalje je $3 < 11$ pa stavljamo $x_2 = 0$ i na kraju je $3 \geq 3$ pa stavljamo $x_1 = 1$. Uočimo da je S na samom kraju reduciran do $3 - 3 = 0$, što nam govori da je rješenje $x = (1, 0, 1, 0, 1)$. Provjerimo:

$$1 \cdot 3 + 0 \cdot 11 + 1 \cdot 24 + 0 \cdot 50 + 1 \cdot 115 = 142. \qquad \checkmark$$

Merkle i Hellman su uveli kriptosustav s javnim ključem baziran na superrastućem problemu sume podskupa koji je zamaskiran pomoću kongruencija. Kako bi kreirala javni/tajni par ključeva, Ana počinje sa superrastućim nizom $r = (r_1, \ldots, r_n)$. Također, odabire dva velika tajna cijela broja A i B koji zadovoljavaju

$$B > 2r_n \qquad \text{i} \qquad (A, B) = 1.$$

Ana zatim kreira novi niz M koji nije superrastući postavljanjem

$$M_i \equiv Ar_i \pmod{B}, \qquad \text{gdje je} \qquad 0 \leq M_i < B.$$

Dobiveni niz M je Anin javni ključ.

Kako bi šifrirao poruku, Ivan odabire otvoreni tekst x koji je binarni vektor te izračunava i šalje Ani šifrat

$$S = x \cdot M = \sum_{i=1}^{n} x_i M_i.$$

Ana dešifrira S tako da prvo računa

$$S' \equiv A^{-1}S \pmod{B}, \qquad \text{gdje je} \qquad 0 \leq S' < B.$$

Ana tada rješava problem sume podskupa za S' koristeći brzi algoritam opisan u Propoziciji 5. Razlog učinkovitosti dešifriranja je taj da je S' kongruentno

$$S' \equiv A^{-1}S \equiv A^{-1}\sum_{i=1}^{n} x_i M_i \equiv A^{-1}\sum_{i=1}^{n} x_i A r_i \equiv \sum_{i=1}^{n} x_i r_i \pmod{B}.$$

Zbog pretpostavke da je $B > 2r_n$ i Leme 4, Ana zna da je

$$\sum_{i=1}^{n} x_i r_i \leq \sum_{i=1}^{n} r_i < 2r_n < B,$$

pa odabirom S' u rasponu od 0 do $B - 1$ osigurava dobivanje ne samo kongruencije nego točne jednakosti $S' = \sum x_i r_i$. Merkle-Hellman kriptosustav sažet je u Tablici 2 ([3, Table 6.2]).

Ana	Ivan
Kreiranje ključa	
Odabire superrastući $r = (r_1, \ldots, r_n)$ te A i B t.d. $B > 2r_n$ i $(A, B) = 1$. Računa $M_i \equiv Ar_i \pmod{B}$ za $1 \leq i \leq n$. Objavljuje javni ključ $M = (M_1, \ldots, M_n)$.	
Enkripcija	
	Odabire binarni otvoreni tekst x. Pomoću Aninog javnog ključa M računa šifrat $S = x \cdot M$ i šalje ga Ani.
Dekripcija	
Računa $S' \equiv A^{-1}S \pmod{B}$. Rješava problem sume podskupova S' koristeći superrastući niz r. Otvoreni tekst x zadovoljava jednakost $x \cdot r = S'$.	

Tablica 2: Merkle-Hellman kriptosustav s problemom sume podskupa

Primjer 7. ([3, Example 6.7.]) Neka je $r = (3, 11, 24, 50, 115)$ Anin tajni superrastući niz i pretpostavimo da je odabrala $A = 113$ i $B = 250$. Tada je njezin zamaskirani niz

$$\begin{aligned} M &\equiv (113 \cdot 3, 113 \cdot 11, 113 \cdot 24, 113 \cdot 50, 113 \cdot 115) \pmod{250} \\ &= (89, 243, 212, 150, 245). \end{aligned}$$

Uočimo, čak i da Ana permutira članove u M na način da poredak bude rastući, ni tada M neće niti izbliza biti superrastući. Ivan odlučuje poslati Ani tajnu poruku $x = (1, 0, 1, 0, 1)$. Šifrira x računanjem

$$S = x \cdot M = 1 \cdot 89 + 0 \cdot 243 + 1 \cdot 212 + 0 \cdot 150 + 1 \cdot 245 = 546.$$

Nakon primitka šifrata S, Ana množi sa 177, jer je to inverz od 113 modulo 250. Time dobiva

$$S' \equiv 177 \cdot 546 = 142 \pmod{250}.$$

Nakon toga, Ana koristi algoritam iz Propozicije 5. kako bi riješila $S' = x \cdot r$ za superrastući niz r. Na taj način je otkrila otvoreni tekst x.

Kriptosustavi bazirani na zamaskiranim problemima sume podskupova poznati su kao *kriptosustavi sume podskupova* ili *kriptosustavi naprtnjače*. Općenito, ideja je započeti s tajnim superrastućim nizom, zamaskirati ga koristeći tajne modularne linearne operacije i objaviti zamaskirani niz kao javni ključ. Originalni Merkle-Hellman sustav predlagao je primjenu tajne permutacije komponenata od $Ar \pmod{B}$ radi dodatne zaštite. Kasnije verzije,

koje su ponudili brojni drugi, uključivale su višestruka množenja i redukcije modulo nekoliko različitih brojeva. Izvrstan pregled kriptosustava naprtnjače može se naći u [6].

Napomena 8. Važno pitanje koje moramo razmotriti u vezi problema naprtnjače je veličina određenih parametara potrebnih za postizanje željene razine sigurnosti. Postoji 2^n binarnih vektora $x = (x_1, \ldots, x_n)$, a u Propoziciji 3. smo vidjeli da se kolizijskim algoritmom problem naprtnjače može reducirati na $\mathcal{O}(2^{n/2})$ operacija. Stoga je za postizanje sigurnosti reda 2^k nužno uzeti $n > 2k$. Primjerice, sigurnost reda 2^{80} zahtijeva $n > 160$. No, iako ovo omogućuje sigurnost protiv kolizijskog napada, ne isključuje postojanost drugih, učinkovitijih napada. Takvi napadi postoje i o njima se više može pronaći u [3, str. 419.]. Također, pročitati Napomenu 10.

Napomena 9. Uz pretpostavku da je n odabran, koje veličine trebaju biti ostali parametri? Ispostavlja se da ako je r_1 suviše mali, može se lako napasti, pa moramo inzistirati da je $r_1 > 2^n$. Kako je niz superrastući, slijedi da je

$$r_n > 2r_{n-1} > 4r_{n-2} > \cdots > 2^n r_1 > 2^{2n}.$$

Tada je $B > 2r_n = 2^{2n+1}$, pa komponente M_i javnog ključa i šifrat S zadovoljavaju

$$M_i = \mathcal{O}(2^{2n}) \qquad i \qquad S = \mathcal{O}(2^{2n}).$$

Slijedi da je javni ključ M lista od n prirodnih brojeva, od kojih je svaki približno $2n$ bitova dug, dok se otvoreni tekst x sastoji od n bitova informacije, a šifrat od približno $2n$ bitova. Uočimo da je omjer proširenja poruke 2 naprema 1.

Primjerice, uzmimo $n = 160$. Tada je veličina javnog ključa oko $2n^2 = 51200$ bitova. Usporedimo li ovo s RSA ili Diffie-Hellman kriptosustavom, gdje je za sigurnost reda 2^{80} veličina javnog ključa samo oko 1000 bitova, to se čini kao golem nedostatak. Međutim, taj nedostatak se kompenzira kroz veliku brzinu sustava naprtnjače. Naime, dekripcija u ovom sustavu zahtijeva samo jedno ili mali broj modularnih množenja, dok enkripcija ne zahtijeva niti jedno. Ovo je mnogo učinkovitije od velikog broja računalno intenzivnih modularnih eksponencijacija korištenih u RSA i Diffie-Hellman kriprosustavu. Upravo je to razlog što su kriptosustavi naprtnjače kroz povijest bili privlačniji.

Napomena 10. Najpoznatiji algoritmi za rješavanje slučajno odabranog problema sume podskupova su verzije kolizijskog algoritma iz Propozicije 3. Nažalost, slučajno odabran problem sume podskupova nema zamke, pa se ne može koristiti za konstrukciju kriptosustava. Ispostavlja se da korištenje zamaskiranih superrastućih problema sume podskupova dopušta i druge, učinkovitije algoritme. Prvi takvi napadi (Shamir, Odlyzko, Lagarias i drugi) koristili su razne ad hoc metode. Objavom poznatog LLL (A.K. Lenstra, H.W. Lenstra, L. Lovasz) rada [4] o redukciji rešetke 1982. godine postalo je jasno da kriptosustavi bazirani na problemu naprtnjače imaju fundamentalnu slabost. Ugrubo, ako je $n < 300$, onda redukcija rešetke omogućuje napadaču oporavak otvorenog teksta x iz šifrata S u uznemirujuće

kratkom vremenu. Stoga siguran sustav zahtijeva $n > 300$, a u tom je slučaju duljina tajnog ključa veća od $2n^2 = 180000$ bitova ≈ 176 KB. Ova veličina čini sigurne kriptosustave naprtnjače nepraktičnima.

Opišimo sada kako Marija može reformulirati problem sume podskupova koristeći vektore. Pretpostavimo da ona želi zapisati S kao sumu podskupova od $M = (m_1, \ldots, m_n)$. Prvi korak je načiniti matricu

$$\begin{bmatrix} 2 & 0 & 0 & \cdots & 0 & m_1 \\ 0 & 2 & 0 & \cdots & 0 & m_2 \\ 0 & 0 & 2 & \cdots & 0 & m_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 2 & m_n \\ 1 & 1 & 1 & \cdots & 1 & S \end{bmatrix}. \tag{4}$$

Bitni vektori ovdje su nam retci matrice (4). Označimo ih s

$$\begin{aligned} v_1 &= (2, 0, 0, \ldots, 0, m_1), \\ v_2 &= (0, 2, 0, \ldots, 0, m_2), \\ &\vdots \\ v_n &= (0, 0, 0, \ldots, 2, m_n), \\ v_{n+1} &= (1, 1, 1, \ldots, 1, S). \end{aligned}$$

Kao i u dvodimenzionalnom primjeru opisanom na kraju prvog poglavlja, Marija razmatra skup svih cjelobrojnih linearnih kombinacija od $v_1, \ldots, v_{n+1}$, tj.

$$L = \{a_1 v_1 + a_2 v_2 + \cdots + a_n v_n + a_{n+1} v_{n+1} \quad : \quad a_1, a_2, \ldots, a_n, a_{n+1} \in \mathbb{Z}\}.$$

Skup L je još jedan primjer *rešetke*.

Pretpostavimo sada da je $x = (x_1, \ldots, x_n)$ rješenje zadanog problema sume podskupova. Tada se u rešetci L nalazi vektor

$$t = \sum_{i=1}^{n} x_i v_i - v_{n+1} = (2x_1 - 1, 2x_2 - 1, \ldots, 2x_n - 1, 0),$$

gdje je zadnja komponenta od t jednaka 0 jer je $S = x_1 m_1 + \cdots + x_n m_n$.

Došli smo do suštine problema. S obzirom da su svi x_1 jednaki 0 ili 1, sve vrijednosti $2x_i - 1$ su jednake ± 1, pa je vektor t poprilično kratak, tj. $||t|| = \sqrt{n}$. S druge strane, vidjeli smo da je $m_i = \mathcal{O}(2^{2n})$ i $S = \mathcal{O}(2^{2n})$, pa svi vektori koji generiraju L imaju duljine $||v_i|| = \mathcal{O}(2^{2n})$. Stoga je malo vjerojatno da L sadrži neke nenul vektore (osim t) čija je duljina mala kao $\sqrt{n}$. Dakle, uz pretpostavku da Marija zna nekim algoritmom pronaći mali nenul vektor u rešetci, ona može pronaći t i potom rekonstruirati otvoreni tekst x.

Algoritmi koji se bave traženjem kratkih vektora u rešetkama zovu se *algoritmi redukcije rešetke*. Najpoznatiji takav je ranije spomenuti LLL algoritam i njegove varijante poput LLL-BKZ. Detaljnije o njima može se naći u [3, str. 419.]. Vidjeti i Primjer 33. u [3, str. 378.].

3 Kratak pregled vektorskih prostora

Prije nego što započnemo raspravu o rešetkama, zaustavit ćemo se i prisjetiti važnih definicija i ideja iz linearne algebre. Iako se vektorski prostori mogu definirati općenitije, za potrebe ovog rada dovoljno je promotriti vektorske prostore sadržane u $\mathbb{R}^m$ za neki prirodni broj m. Započet ćemo s osnovnim definicijama potrebnim za proučavanje vektorskih prostora.

Vektorski prostor. ([3, Poglavlje 6]) *Vektorski prostor* V je podskup od $\mathbb{R}^m$ sa svojstvom

$$\alpha_1 v_1 + \alpha_2 v_2 \in V, \qquad \forall v_1, v_2 \in V \quad \text{i} \quad \forall \alpha_1, \alpha_2 \in \mathbb{R}.$$

Ekvivalentno, vektorski prostor je podskup od $\mathbb{R}^m$ zatvoren na zbrajanje i množenje skalarima iz $\mathbb{R}$.

Linearna kombinacija. ([3, Poglavlje 6]) Neka su $v_1, v_2, \ldots, v_k \in V$. *Linearna kombinacija* vektora $v_1, v_2, \ldots, v_k \in V$ je bilo koji vektor oblika

$$w = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k, \qquad \text{gdje su} \qquad \alpha_1, \ldots, \alpha_k \in \mathbb{R}.$$

Skup svih takvih linearnih kombinacija,

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

nazivamo *linearna ljuska* skupa $\{v_1, \ldots, v_k\}$.

Nezavisnost. ([3, Poglavlje 6]) Skup vektora $v_1, v_2, \ldots, v_k \in V$ je linearno nezavisan ako

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = 0 \tag{5}$$

povlači da je $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$. Skup je linearno zavisan ako možemo postići jednakost (5) uz barem jedan $\alpha_i \neq 0$.

Baza. ([3, Poglavlje 6]) *Baza* za V je skup linearno nezavisnih vektora $v_1, \ldots, v_n$ čija je linearna ljuska jednaka čitavom V. Ekvivalentno je reći da se svaki vektor $w \in V$ može zapisati u obliku

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

uz jedinstven izbor skalara $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$.

Opišimo sada vezu različitih baza i važnog koncepta dimenzije vektorskog prostora.

Propozicija 11. ([3, Proposition 6.11.]) *Neka je $V \subset \mathbb{R}^m$ vektorski prostor.*
(a) *Postoji baza za V.*
(b) *Bilo koje dvije baze za V imaju isti broj elemenata. Broj elemenata u bazi za V nazivamo* dimenzijom od V.

(c) *Neka je $v_1, \ldots, v_n$ baza za V te neka je $w_1, \ldots, w_n$ neki drugi skup od n vektora u V. Zapišimo svaki w_j kao linearnu kombinaciju vektora v_i,*

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

Tada je $w_1, \ldots, w_n$ također baza za V ako i samo ako je determinanta matrice

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

različita od 0.

Sada ćemo objasniti kako u $\mathbb{R}^n$ mjeriti duljinu vektora. Ovaj važan koncept povezan je sa zapisom skalarnog produkta i euklidske norme.

Skalarni produkt i duljina. ([3, Poglavlje 6]) Neka su $v, w \in V \subset \mathbb{R}^m$ i zapišimo v i w pomoću koordinata kao

$$v = (x_1, x_2, \ldots, x_m) \qquad i \qquad w = (y_1, y_2, \ldots, y_m).$$

Skalarni produkt vektora v i w je broj

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

Kažemo da su v i w *(međusobno) okomiti* ako je $v \cdot w = 0$.

Duljina ili *euklidska norma* vektora v je broj

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

Uočimo da su spomenuti skalarni produkt i norma povezani formulom

$$v \cdot v = \|v\|^2.$$

Ortogonalnost. ([3, Poglavlje 6]) *Ortogonalna baza* za vektorski prostor V je baza $v_1, \ldots, v_n$ sa svojstvom

$$v_i \cdot v_j = 0 \qquad \text{za sve} \qquad i \neq j.$$

Baza je *ortonormirana* ako dodatno vrijedi $\|v_i\| = 1, \quad \forall i$.

Mnoge se formule korištenjem ortogonalne ili ortonormirane baze pojednostavljuju. Na primjer, ako je $v_1, \ldots, v_n$ ortogonalna baza i ako je $v = a_1v_1 + \cdots + a_nv_n$ linearna kombinacija baznih vektora, tada je

$$\begin{aligned}\|v\|^2 &= \|a_1v_1 + \cdots + a_nv_n\|^2 \\ &= (a_1v_1 + \cdots + a_nv_n) \cdot (a_1v_1 + \cdots + a_nv_n) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_ia_j(v_i \cdot v_j) \\ &= \sum_{i=1}^{n} a_i^2\|v_i\|^2 \qquad \text{jer je} \qquad v_i \cdot v_j = 0 \qquad \text{za} \qquad i \neq j.\end{aligned}$$

Ako je baza ortonormirana, ovo se dalje pojednostavljuje na $\|v\|^2 = \sum a_i^2$.

Za konstrukciju ortonormirane baze postoji standardna metoda koju nazivamo Gram-Schmidtov algoritam. Opišimo jednu varijantu uobičajenog algoritma koji daje ortogonalnu bazu.

Teorem 12. (Gram-Schmidtov algoritam) ([3, Theorem 6.13.]) *Neka je $v_1, \ldots, v_n$ baza za vektorski prostor $V \subset \mathbb{R}^m$. Sljedeći algoritam daje ortogonalnu bazu $v_1^*, \ldots, v_n^*$ za V:*

Postavi $v_1^* = v_1$.
Za $i = 2, 3, \ldots, n$
Računaj $\mu_{ij} = v_i \cdot v_j^*/\|v_j^*\|^2$ za $1 \leq j < i$.
Postavi $v_i^* = v_i - \sum_{j=1}^{i-1} \mu_{ij}v_j^*$.

Za spomenute dvije baze vrijedi

$$[\{v_1, \ldots, v_i\}] = [\{v_1^*, \ldots, v_i^*\}], \qquad \forall i = 1, 2, \ldots, n.$$

Dokaz. Ortogonalnost dokazujemo indukcijom. Pretpostavimo da su vektori $v_1^*, \ldots, v_{i-1}^*$ u parovima ortogonalni. Trebamo dokazati da je vektor v_i^* ortogonalan na sve njih. Uzmemo bilo koji $k < i$ i računamo

$$\begin{aligned}v_i^* \cdot v_k^* &= \left(v_i - \sum_{j=1}^{i-1} \mu_{ij}v_j^*\right) \cdot v_k^* \\ &= v_i \cdot v_k^* - \mu_{ik}\|v_k^*\|^2 \qquad \text{jer je} \quad v_k^* \cdot v_j^* = 0 \quad \text{za} \quad j \neq k, \\ &= 0 \qquad \text{po definiciji} \quad \mu_{ik}.\end{aligned}$$

Radi dokazivanja posljednje tvrdnje o linearnim ljuskama, prvo uočimo da je iz definicije v_i^* jasno kako je v_i u linearnoj ljusci vektora $v_1^*, \ldots, v_i^*$. Obratnu inkluziju dokazujemo indukcijom. Pretpostavimo da su $v_1^*, \ldots, v_{i-1}^*$ u linearnoj ljusci vektora $v_1, \ldots, v_{i-1}$. Treba dokazati da je v_i^* u linearnoj ljusci od $v_1, \ldots, v_i$. Po definiciji v_i^* jasno je da je on u linearnoj ljusci vektora $v_1^*, \ldots, v_{i-1}^*, v_i$ pa samo primijenimo pretpostavku indukcije. $\square$

4 Rešetke: Osnovne definicije i svojstva

Nakon primjera u prvom i drugom poglavlju te ponavljanja temeljnih svojstava vektorskih prostora u trećem poglavlju, slijede formalne definicije rešetke i pregled njezinih svojstava.

Definicija. ([3, Poglavlje 6]) Neka je $v_1, \ldots, v_n \in \mathbb{R}^m$ linearno nezavisan skup vektora. *Rešetka L generirana vektorima $v_1, \ldots, v_n$* je skup svih linearnih kombinacija vektora $v_1, \ldots, v_n$ s koeficijentima iz $\mathbb{Z}$, tj.

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

Baza za L je bilo koji linearno nezavisan skup vektora koji generira L. Bilo koja dva takva skupa imaju isti broj elemenata. Broj vektora u bazi za L nazivamo *dimenzijom od L*.

Pretpostavimo da je $v_1, \ldots, v_n$ baza za rešetku L i da je $w_1, \ldots, w_n \in L$ neki drugi skup vektora iz L. Kao što smo učinili kod vektorskih prostora, možemo zapisati svaki w_j kao linearnu kombinaciju baznih vektora, tj.

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

no sada znamo da su svi koeficijenti a_{ij} cjelobrojni jer je L rešetka.

Pretpostavimo da želimo izraziti vektore v_i pomoću vektora w_j. Tada je potrebno invertirati matricu

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

Uočimo da želimo v_i izraziti kao linearne kombinacije od w_j koristeći *cjelobrojne* koeficijente, pa komponente matrice A^{-1} trebaju biti cjelobrojne. Dakle,

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

gdje su $\det(A)$ i $\det(A^{-1})$ cijeli brojevi, pa mora slijediti $\det(A) = \pm 1$. Obratno, ukoliko je $\det(A) = \pm 1$, tada nam teorija adjungirane matrice govori da A^{-1} uistinu ima cjelobrojne komponente. Ovo zapravo dokazuje sljedeći koristan rezultat.

Propozicija 13. ([3, Proposition 6.14.]) *Bilo koje dvije baze za rešetku L povezane su matricom s cjelobrojnim komponentama i determinantom jednakom ± 1.*

U svrhu računanja, obično je prikladno raditi s rešetkama čiji vektori imaju cjelobrojne koordinate. Primjerice,

$$\mathbb{Z}^n = \{(x_1, x_2, \ldots, x_n); x_1, x_2, \ldots, x_n \in \mathbb{Z}\}$$

je rešetka koja sadrži sve vektore s cjelobrojnim komponentama.

Definicija. ([3, Poglavlje 6]) *Cjelobrojna (ili integralna) rešetka* je rešetka kojoj svi vektori imaju cjelobrojne komponente. Ekvivalentno, cjelobrojna rešetka je aditivna podgrupa od $\mathbb{Z}^m$ za neki $m \geq 1$.

Primjer 14. ([3, Example 6.15.]) Promotrimo trodimenzionalnu rešetku $L \subset \mathbb{R}^3$ generiranu trima vektorima

$$v_1 = (2, 1, 3), \quad v_2 = (1, 2, 0), \quad v_3 = (2, -3, -5).$$

Prikladno je načiniti matricu koristeći vektore v_1, v_2, v_3 kao retke te matrice, dakle

$$A = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 2 & -3 & -5 \end{bmatrix}.$$

Konstruirajmo tri nova vektora u L na sljedeći način:

$$w_1 = v_1 + v_3, \qquad w_2 = v_1 - v_2 + 2v_3, \qquad w_3 = v_1 + 2v_2.$$

Ovo je ekvivalentno množenju matrice A slijeva matricom

$$U = \begin{bmatrix} 1 & 0 & 1 \\ 1 & -1 & 2 \\ 1 & 2 & 0 \end{bmatrix},$$

pa dobivamo da su w_1, w_2, w_3 retci matrice

$$B = UA = \begin{bmatrix} 4 & -2 & -2 \\ 5 & -7 & -7 \\ 4 & 5 & 3 \end{bmatrix}.$$

Matrica U ima determinantu -1, pa su vektori w_1, w_2, w_3 također baza za L. Inverz od U je

$$U^{-1} = \begin{bmatrix} 4 & -2 & -1 \\ -2 & 1 & 1 \\ -3 & 2 & 1 \end{bmatrix},$$

a retci od U^{-1} nam govore kako izraziti v_i kao linearne kombinacije od w_j:

$$v_1 = 4w_1 - 2w_2 - w_3, \quad v_2 = -2w_1 + w_2 + w_3, \quad v_3 = -3w_1 + 2w_2 + w_3.$$

Napomena 15. Ako je $L \subset \mathbb{R}^m$ rešetka dimenzije n, onda bazu za L možemo zapisati kao retke matrice A dimenzije $n \times m$, odnosno matrice koja ima n redaka i m stupaca. Nova baza za L može se dobiti množenjem matrice A slijeva matricom U dimenzije $n \times n$, pri čemu su komponente od U cjelobrojne, a determinanta joj je ± 1. Skup takvih matrica U nazivamo *općom linearnom grupom nad* $\mathbb{Z}$ i označavamo s $\mathrm{GL}_n(\mathbb{Z})$. To je zapravo grupa matrica s cjelobrojnim komponentama čiji inverzi također imaju cjelobrojne komponente.

Postoji i alternativni, apstraktniji način definiranja rešetki u kojem se isprepliću algebra i geometrija.

Definicija. ([3, Poglavlje 6]) Podskup $L \subset \mathbb{R}^m$ je *aditivna podgrupa* ako je zatvoren na operacije zbrajanja i oduzimanja. Nazivamo ga *diskretnom aditivnom podgrupom* ako postoji pozitivna konstanta $\epsilon > 0$ za koju vrijedi sljedeće svojstvo: za svaki $v \in L$,

$$L \cap \{w \in \mathbb{R}^m : \|v - w\| < \epsilon\} = \{v\}. \tag{6}$$

Drugim riječima, uzmemo li bilo koji vektor $v \in L$ i oko njega opišemo otvorenu kuglu polumjera ϵ, tada unutar te kugle nema drugih točaka iz L.

Ovu definiciju opravdava sljedeći teorem, čiji dokaz izostavljamo. Vidjeti [1, str. 423., Exercise 6.9].

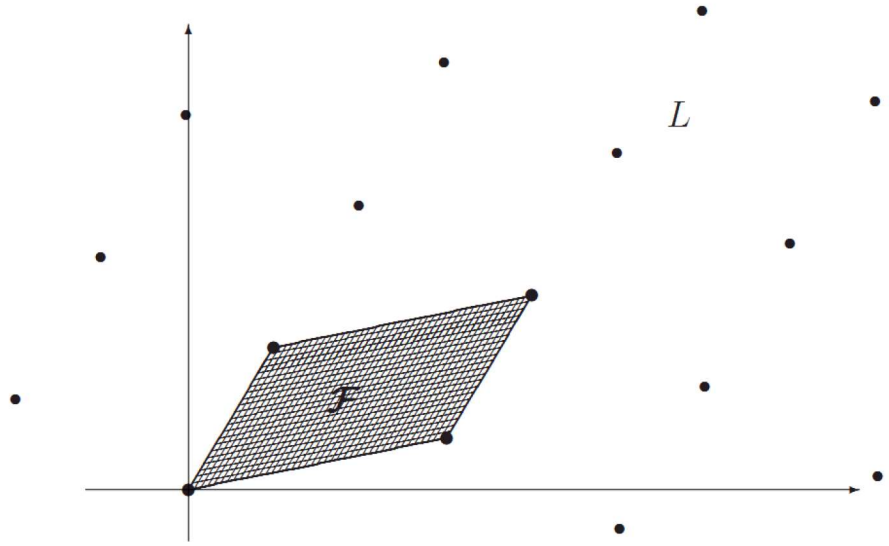
Teorem 16. ([3, Theorem 6.17.]) *Podskup od* $\mathbb{R}^m$ *je rešetka ako i samo ako je taj podskup diskretna aditivna podgrupa.*

Rešetka je slična realnom vektorskom prostoru. Razlika je ta da se ne konstruira svim linearnim kombinacijama baznih vektora s proizvoljnim realnim koeficijentima, već samo s cjelobrojnim koeficijentima. Korisno je rešetku predočiti kao uređen poredak točaka u $\mathbb{R}^m$ na način da točku stavimo u kraj svakog vektora. Primjer rešetke u $\mathbb{R}^2$ ilustriran je na Slici 1 ([3, Figure 6.1]).

Definicija. ([3, Poglavlje 6]) Neka je L rešetka dimenzije n s bazom $v_1, v_2, \ldots, v_n$. *Fundamentalna domena* (ili *fundamentalni paralelepiped*) za L koji odgovara ovoj bazi je skup

$$\mathcal{F}(v_1, v_2, \ldots, v_n) = \{t_1 v_1 + t_2 v_2 + \cdots + t_n v_n : 0 \leq t_i < 1\}. \tag{7}$$

Osjenčano područje na Slici 1 prikazuje fundamentalnu domenu u dvodimenzionalnom slučaju. Sljedeći rezultat ukazuje na jedan od razloga zašto su fundamentalne domene važne u proučavanju rešetaka.



Slika 1: Rešetka L i fundamentalna domena $\mathcal{F}$

Propozicija 17. ([3, Proposition 6.18.]) *Neka je $L \subset \mathbb{R}^n$ rešetka dimenzije n i neka je $\mathcal{F}$ njezina fundamentalna domena. Tada se svaki vektor $w \in \mathbb{R}^n$ može zapisati u obliku*

$$w = t + v$$

za jedinstven $t \in \mathcal{F}$ i za jedinstven $v \in L$. Ekvivalentno, unija translatiranih fundamentalnih domena

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

gdje se v kreće po svim vektorima rešetke L, egzaktno pokriva $\mathbb{R}^n$.

Demonstracija ovog rezultata u dvodimenzionalnom slučaju može se vidjeti na Slici 2. ([3, Figure 6.2]), a u nastavku slijedi dokaz za n-dimenzionalan slučaj.

Dokaz. Neka je $v_1, \ldots, v_n$ baza za L kojoj odgovara fundamentalna domena $\mathcal{F}$. Kako su $v_1, \ldots, v_n$ linearno nezavisni u $\mathbb{R}^n$, oni čine bazu za $\mathbb{R}^n$. To znači da se svaki $w \in \mathbb{R}^n$ može zapisati u obliku

$$w = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n,$$

za neke $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$. Zapišimo sada svaki α_i kao

$$\alpha_i = t_i + a_i, \qquad \text{gdje je} \quad 0 \leq t_i < 1 \quad \text{i} \quad a_i \in \mathbb{Z}.$$

Tada je

$$w = (t_1 v_1 + t_2 v_2 + \cdots + t_n v_n) + (a_1 v_1 + a_2 v_2 + \cdots + a_n v_n),$$

gdje je vektor u prvoj zagradi $t \in \mathcal{F}$, a vektor u drugoj zagradi $v \in L$, odnosno w se može prikazati u željenom zapisu.

Nadalje pretpostavimo da w ima dva prikaza u obliku sume jednoga vektora iz $\mathcal{F}$ i jednoga iz L, odnosno $w = t + v = t' + v'$. Tada je

$$(t_1 + a_1)v_1 + (t_2 + a_2)v_2 + \cdots + (t_n + a_n)v_n$$
$$= (t'_1 + a'_1)v_1 + (t'_2 + a'_2)v_2 + \cdots + (t'_n + a'_n)v_n.$$

Zbog linearne nezavisnosti vektora $v_1, \ldots, v_n$, slijedi da je

$$t_i + a_i = t'_i + a'_i, \qquad \text{za sve} \quad i = 1, 2, \ldots, n.$$

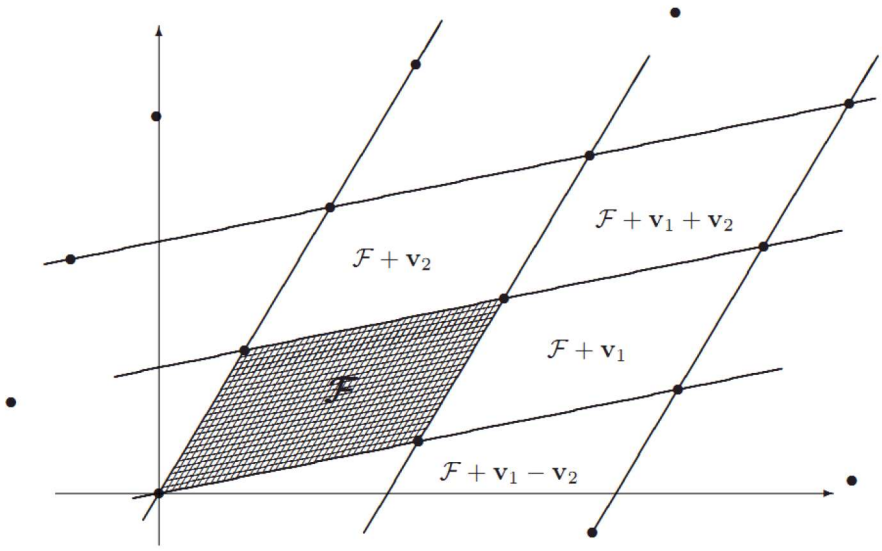
Stoga je

$$t_i - t'_i = a'_i - a_i \in \mathbb{Z}$$

cijeli broj. S obzirom da znamo da su t_i i t'_i veći ili jednaki 0 i strogo manji od 1, jedini način da razlika $t_i - t'_i$ bude cjelobrojna je ako vrijedi $t_i = t'_i$. Zbog toga je $t = t'$ i zatim

$$v = w - t = w - t' = v'.$$

Ovime je dokazano da su $t \in \mathcal{F}$ i $v \in L$ vektorom w jedinstveno određeni. □



Slika 2: Translacije $\mathcal{F}$ vektorima iz L egzaktno pokrivaju $\mathbb{R}^n$

Ispostavlja se da sve fundamentalne domene rešetke L imaju isti volumen. Ovo ćemo dokazati malo poslije, u Korolaru 21., za rešetke dimenzije n u $\mathbb{R}^n$. Volumen fundamentalne domene je vrlo važna invarijanta rešetke.

Definicija. ([3, Poglavlje 6]) Neka je L rešetka dimenzije n te $\mathcal{F}$ njezina fundamentalna domena. Tada n-dimenzionalni volumen od $\mathcal{F}$ nazivamo *determinantom rešetke* L (katkada i *kovolumenom* od L). Označavamo s $\det(L)$.

Rešetka L sama po sebi nema volumen, jer je riječ o prebrojivom skupu točaka. Ako je $L \subset \mathbb{R}^n$ dimenzije n, tada je *kovolumen* od L definiran kao volumen kvocijentne grupe $\mathbb{R}^n/L$.

Ako zamišljamo bazne vektore $v_1, \ldots, v_n$ kao vektore zadane duljine koji opisuju strane parelelepipeda $\mathcal{F}$, tada se za bazne vektore zadanih duljina najveći volumen postiže ako su vektori u parovima međusobno okomiti. Ovo nas dovodi do sljedeće važne gornje ograde za determinantu rešetke.

Propozicija 18. ([3, Proposition 6.19.]) (Hadamardova nejednakost) *Neka je L rešetka, $v_1, \ldots, v_n$ bilo koja baza za L te $\mathcal{F}$ fundamentalna domena za L. Tada je*

$$\det L = \mathrm{Vol}(\mathcal{F}) \leq \|v_1\| \, \|v_2\| \cdots \|v_n\|. \tag{8}$$

Što je baza bliža ortogonalnoj, to je Hadamardova nejednakost (8) bliža jednakosti.

Prilično je jednostavno izračunati determinantu rešetke L ako joj je dimenzija jednaka dimenziji ambijentnog prostora, tj. ako je L sadržana u $\mathbb{R}^n$ i ako L ima dimenziju n. Srećom, ovakav slučaj nam i jest od najvećeg interesa, a formula potrebna za računanje opisana je u sljedećoj propoziciji.

Propozicija 19. ([3, Proposition 6.20.]) *Neka je $L \subset \mathbb{R}^n$ rešetka dimenzije n, $v_1, v_2, \ldots, v_n$ baza za L te $\mathcal{F} = \mathcal{F}(v_1, \ldots, v_n)$ pripadna fundamentalna domena kako je definirano u (7). Zapišimo koordinate i-tog baznog vektora kao*

$$v_i = (r_{i1}, r_{i2}, \ldots, r_{in})$$

te složimo koordinate od v_i u retke matrice,

$$F = F(v_1, \ldots, v_n) = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} \end{bmatrix}. \tag{9}$$

Tada je volumen od $\mathcal{F}$ dan formulom

$$\mathrm{Vol}(\mathcal{F}(v_1, \ldots, v_n)) = |\det(F(v_1, \ldots, v_n))|.$$

Dokaz. Potreban nam je diferencijalni račun više varijabli. Volumen od $\mathcal{F}$ možemo računati kao integral konstantne funkcije 1 po području $\mathcal{F}$, odnosno

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

Fundamentalna domena $\mathcal{F}$ je skup opisan s (7), pa ćemo promijeniti varijable integracije iz $x = (x_1, \dots, x_n)$ u $t = (t_1, \dots, t_n)$ koristeći se formulom

$$(x_1, x_2, \dots, x_n) = t_1 v_1 + t_2 v_2 + \cdots + t_n v_n.$$

U terminima matrice $F = F(v_1, \dots, v_n)$ definirane s (9), zamjena varijabli zadana je matričnom jednadžbom $x = tF$. F je zapravo Jakobijan za ovu zamjenu varijabli, a fundamentalna domena $\mathcal{F}$ je dobivena djelovanjem od F na jediničnu n-dimenzionalnu hiperkocku $C_n = [0,1]^n$. Po formuli za zamjenu varijabli u integralu stoga imamo

$$\begin{aligned}\int_{\mathcal{F}} dx_1 dx_2 \dots dx_n &= \int_{FC_n} dx_1 dx_2 \dots dx_n \\ &= \int_{C_n} |\det F| dt_1 dt_2 \dots dt_n \\ &= |\det F| \mathrm{Vol}(C_n) \\ &= |\det F|. \qquad \square\end{aligned}$$

Primjer 20. ([3, Example 6.21.]) Rešetka u Primjeru 15. ima determinantu

$$\det L = |\det A| = \left| \det \begin{bmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 2 & -3 & -5 \end{bmatrix} \right| = |-36| = 36.$$

Korolar 21. ([3, Corollary 6.22.]) *Neka je L rešetka dimenzije n. Tada sve fundamentalne domene za L imaju isti volumen. Dakle,* $\det L$ *je invarijanta rešetke L, neovisna o tome koju smo fundamentalnu domenu koristili za izračun.*

Dokaz. Neka su $v_1, \dots, v_n$ i $w_1, \dots, w_n$ dvije fundamentalne domene za L te neka su $F(v_1, \dots, v_n)$ i $F(w_1, \dots, w_n)$ pripadne matrice dobivene slaganjem koordinata vektora u retke matrica kao u (9). Zbog Propozicije 14. vrijedi

$$F(v_1, \dots, v_n) = AF(w_1, \dots, w_n) \tag{10}$$

za neku $n \times n$ matricu A kojoj su komponente cjelobrojne i $\det(A) = \pm 1$. Primjenivši Propoziciju 20. dvaput, dobivamo:

$\mathrm{Vol}(\mathcal{F}(v_1, \ldots, v_n))$

$= |\det(F(v_1, \ldots, v_n))|$ zbog Propozicije 20.,

$= |\det(AF(w_1, \ldots, w_n))|$ zbog (10),

$= |\det(A)|\,|\det(F(w_1, \ldots, w_n))|$ jer je $\det(AB) = \det(A)\det(B)$,

$= |\det(F(w_1, \ldots, w_n))|$ jer je $\det(A) = \pm 1$,

$= \mathrm{Vol}(\mathcal{F}(w_1, \ldots, w_n))$ zbog Propozicije 20. $\square$

5 Kratki vektori u rešetkama

Temeljni računski problemi povezani s rešetkama su pronalazak najkraćeg nenul vektora u rešetci te pronalazak vektora u rešetci najbližeg nekom zadanom vektoru koji nije u toj rešetci. U ovom poglavlju raspravljamo o tim problemima, uglavnom s teorijske perspektive. O praktičnim metodama za pronalazak kratkih i bliskih vektora u rešetci može se više pronaći u [1, str. 403.-418.].

5.1 Problem najkraćeg i problem najbližeg vektora

Započnimo s opisom ovih dvaju temeljnih problema rešetaka:

Problem najkraćeg vektora (The Shortest Vector Problem, SVP): Treba pronaći najkraći nenul vektor u rešetci L, tj. pronaći nenul vektor $v \in L$ koji minimizira euklidsku normu $\|v\|$.

Problem najbližeg vektora (The Closest Vector Problem, CVP): Za zadani vektor $w \in \mathbb{R}^m$ koji nije u L, treba pronaći vektor $v \in L$ koji je najbliži w, odnosno pronaći vektor $v \in L$ koji minimizira euklidsku normu $\|w - v\|$.

Napomena 22. Uočimo da može postojati više najkraćih nenul vektora u rešetci. Primjerice, u $\mathbb{Z}^2$, sva četiri vektora $(0, \pm 1)$ i $(\pm 1, 0)$ su rješenja za SVP. Zato SVP podrazumijeva traženje nekog najkraćeg vektora, ne nužno jedinstvenog. Slična napomena vrijedi i za CVP.

U prva dva poglavlja vidjeli smo da se rješenje SVP može koristiti za probijanje različitih kriptosustava. Poslije ćemo navesti još neke primjere.

SVP i CVP su duboki problemi i oba postaju računalno teški povećanjem dimenzije rešetke n. U drugu ruku, pokazuje se da čak i aproksimativna rješenja za SVP i CVP imaju iznenađujuće mnogo primjena u različitim područjima čiste i primijenjene matematike. U punoj općenitosti, CVP se smatra $\mathcal{NP}$-teškim problemom, dok je SVP $\mathcal{NP}$-težak pod određenom pretpostavkom randomizirane redukcije. Pretpostavka je, naime, da klasu algoritama s polinomijalnim vremenom izvršenja proširujemo tako da uključuje i one koji nisu deterministički, ali će s visokom vjerojatnošću terminirati u polinomijalnom vremenu s točnim rezultatom. O ovome se više može pronaći u [1].

U praksi, CVP se smatra nešto težim problemom od SVP, jer se CVP obično može reducirati na SVP u nešto većoj dimenziji. Primjerice, $(n+1)$-dimenzionalan SVP korišten za rješavanje kriptosustava naprtnjače u drugom poglavlju može se prirodno formulirati kao n-dimenzionalan CVP. Dokaz da SVP nije teži od CVP može se naći u [2], dok se temeljita rasprava o složenosti različitih problema rešetaka može naći u [5].

Napomena 23. U punoj općenitosti, i SVP i CVP smatramo ekstremno teškim problemima, no u praksi je teško postići idealnu "punu općenitost". U stvarnosti, kriptosustavi bazirani na $\mathcal{NP}$-teškim ili $\mathcal{NP}$-potpunim problemima oslanjaju se na određenu podklasu problema, bilo radi postizanja učinkovitosti ili radi konstrukcije zamke. Na takav način, uvijek postoji mogućnost da neko posebno svojstvo odabrane podklase problema dopušta lakše rješavanje nego u općenitom slučaju. S ovim smo se već susreli u kriptosustavu naprtnjače u drugom poglavlju. Općenit problem naprtnjače je $\mathcal{NP}$-potpun, ali je zamaskirani superrastući problem naprtnjače predložen za korištenje u kriptografiji mnogo lakše riješiti.

Mnogo je važnih varijanti SVP i CVP koji izviru i iz teorije i iz primjene. U nastavku ćemo opisati neke od njih.

Problem najkraće baze (Shortest Basis Problem, SBP) Treba pronaći bazu $v_1, \ldots, v_n$ za rešetku koja je najkraća (u nekom smislu). Zahtjev, naprimjer, može biti minimizacija

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

Očito postoji mnogo različitih verzija za SBP, ovisno o tome kako odaberemo mjeriti "veličinu" baze.

Problem približno najkraćeg vektora (Approximate Shortest Vector Problem, apprSVP) Neka je $\psi(n)$ funkcija od n. U rešetci L dimenzije n treba pronaći nenul vektor koji nije više od $\psi(n)$ puta dulji od najkraćeg nenul vektora. Drugim riječima, ako je $v_{najkraci}$ najkraći nenul vektor u L, tražimo nenul vektor $v \in L$ koji zadovoljava

$$\|v\| \leq \psi(n)\, \|v_{najkraci}\|.$$

Svaki pojedini izbor funkcije $\psi(n)$ daje različit apprSVP. Navedimo dva konkretna primjera. Mogli bismo tražiti algoritam za pronalazak nenul vektora $v \in L$ koji zadovoljava

$$\|v\| \leq 3\sqrt{n}\|v_{najkraci}\| \qquad \text{ili} \qquad \|v\| \leq 2^{n/2}\|v_{najkraci}\|.$$

Jasno je da je algoritam koji rješava prvi problem mnogo snažniji od onog koji rješava drugi problem, no čak se i taj slabiji algoritam može pokazati korisnim ako dimenzija nije prevelika.

Problem približno najbližeg vektora (Approximate Closest Vector Problem, apprCVP) Ovaj problem je isti kao apprSVP, no ovdje tražimo vektor koji je približno rješenje za CVP umjesto SVP.

5.2 Hermiteov teorem i teorem Minkowskog

Koliko je dug najkraći nenul vektor u rešetci L? Odgovor na ovo pitanje donekle ovisi o dimenziji te determinanti od L. Sljedeći rezultat nam eksplicitno daje gornju ogradu za duljinu najkraćeg nenul vektora u rešetci L u terminima $\dim(L)$ i $\det(L)$.

Teorem 24. (Hermiteov teorem) ([3, Theorem 6.25.]) *Svaka rešetka L dimenzije n sadrži nenul vektor $v \in L$ koji zadovoljava*

$$\|v\| \leq \sqrt{n}\det(L)^{1/n}.$$

Napomena 25. Za zadanu dimenziju n, *Hermiteova konstanta* γ_n je najmanja vrijednost za koju svaka rešetka L dimenzije n sadrži nenul vektor $v \in L$ koji zadovoljava

$$\|v\|^2 \leq \gamma_n \det(L)^{2/n}.$$

Naša verzija Hermiteovog teorema govori da je $\gamma_n \leq n$. Točna vrijednost za γ_n poznata je samo za $1 \leq n \leq 8$ i za $n = 24$:

$$\gamma_2^2 = \frac{4}{3}, \qquad \gamma_3^3 = 2, \qquad \gamma_4^4 = 4, \qquad \gamma_5^5 = 8$$

$$\gamma_6^6 = \frac{64}{3}, \qquad \gamma_7^7 = 64, \qquad \gamma_8^8 = 256, \qquad \gamma_{24} = 4.$$

U kriptografske svrhe, posebno nas zanima vrijednost od γ_n za velike n. Za velike n poznato je da Hermiteova konstanta zadovoljava

$$\frac{n}{2\pi e} \leq \gamma_n \leq \frac{n}{\pi e}, \tag{11}$$

gdje su $\pi = 3.14159\ldots$ i $e = 2.71828\ldots$ uobičajene konstante.

Napomena 26. Neke verzije Hermiteovog teorema govore o više vektora. Primjerice, može se dokazati da n-dimenzionalna rešetka L uvijek ima bazu $v_1, \ldots, v_n$ koja zadovoljava

$$\|v_1\|\,\|v_2\| \cdots \|v_n\| \leq n^{n/2}\det(L).$$

Ovo upotpunjuje Hadamardovu nejednakost (Propozicija 19) koja govori da svaka baza zadovoljava

$$\|v_1\|\,\|v_2\| \cdots \|v_n\| \geq \det(L).$$

Definiramo *Hadamardov omjer za bazu* $\mathcal{B} = \{v_1, \ldots, v_n\}$ ([3, Poglavlje 6]) kao vrijednost

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

Vrijedi $0 < \mathcal{H}(\mathcal{B}) \leq 1$, a što je ta vrijednost bliža jedinici, vektori u bazi su ortogonalniji. Spomenimo i to da se recipročna vrijednost Hadamardovog omjera ponekad naziva *defektom ortogonalnosti*.

Dokaz Hermiteovog teorema koristi rezultat Minkowskog koji i samostalno ima veliku važnost. Prije iskaza teorema Minkowskog, uvedimo još neke oznake i osnovne definicije.

Definicija. ([3, Poglavlje 6]) Za proizvoljan $a \in \mathbb{R}^n$ i bilo koji $R > 0$, *(zatvorena) kugla polumjera R sa središtem u a* je skup

$$\mathbb{B}_R(a) = \{x \in \mathbb{R}^n : \|x - a\| \leq R\}.$$

Definicija. ([3, Poglavlje 6]) Neka je S podskup od $\mathbb{R}^n$.

(a) Kažemo da je S *omeđen* ako su duljine vektora u S omeđene. Ekvivalentno, S je omeđen ako postoji radijus R takav da je cijeli S sadržan u kugli $\mathbb{B}_R(0)$.

(b) Kažemo da je S *simetričan* ako je za svaku točku $a \in S$ suprotna točka $-a$ također u S.

(c) Kažemo da je S *konveksan* ako se za bilo koje dvije točke $a, b \in S$ cijela njihova spojnica nalazi u S.

(d) Kažemo da je S zatvoren ako vrijedi sljedeće: ako je $a \in \mathbb{R}^n$ točka takva da svaka kugla $\mathbb{B}_R(a)$ sadrži točku iz S, tada je $a \in S$.

Teorem 27. (Teorem Minkowskog) ([3, Theorem 6.28.]) *Neka je $L \subset \mathbb{R}^n$ rešetka dimenzije n te $S \subset \mathbb{R}^n$ simetričan konveksan skup čiji volumen zadovoljava*

$$\mathrm{Vol}(S) > 2^n \det(L).$$

Tada S sadržava nenul vektor rešetke. Ako je S i zatvoren, tada je dovoljan uvjet

$$\mathrm{Vol}(S) \geq 2^n \det(L).$$

Dokaz. Neka je $\mathcal{F}$ fundamentalna domena za L. Po Propoziciji 17. znamo da se svaki vektor $a \in S$ može na jedinstven način prikazati u obliku

$$a = v_a + w_a, \qquad v_a \in L, \qquad w_a \in \mathcal{F}.$$

(Za ilustraciju pogledati Sliku 2.) Rastegnimo S uz faktor $\frac{1}{2}$, odnosno smanjimo S faktorom 2 na sljedeći način:

$$\frac{1}{2}S = \left\{\frac{1}{2}a : a \in S\right\}.$$

Promotrimo preslikavanje

$$\frac{1}{2}S \to \mathcal{F}, \qquad \frac{1}{2}a \to w_{\frac{1}{2}a}. \tag{12}$$

Ovakvim smanjenjem S faktorom 2 smanjuje mu se volumen faktorom 2^n. Iskoristimo li pretpostavku da je volumen od S veći od $2^n\det(L)$, imamo:

$$\mathrm{Vol}\left(\frac{1}{2}S\right) = \frac{1}{2^n}\mathrm{Vol}(S) > \det(L) = \mathrm{Vol}(\mathcal{F}).$$

Navedeno preslikavanje zadano je kao konačan skup translacija (jer je S omeđen), pa takvo preslikavanje čuva volumen. Činjenica da domena $\frac{1}{2}S$ ovog preslikavanja ima volumen strogo veći od volumena slike $\mathcal{F}$ ovog preslikavanja povlači egzistenciju različitih originala $\frac{1}{2}a_1$ i $\frac{1}{2}a_2$ koji u $\mathcal{F}$ imaju istu sliku.

Dakle, pronašli smo različite točke u S za koje vrijedi

$$\frac{1}{2}a_1 = v_1 + w, \qquad \frac{1}{2}a_2 = v_2 + w, \qquad v_1, v_2 \in L, \quad w \in \mathcal{F}.$$

Oduzmemo li ih, dobivamo nenul vektor

$$\frac{1}{2}a_1 - \frac{1}{2}a_2 = v_1 - v_2 \in L.$$

Zbog simetričnosti skupa S, točka $-a_2$ se nalazi u S. Nadalje, lijeva strana posljednje jednakosti predstavlja polovište spojnice točaka a_1 i $-a_2$, a ono se također nalazi u S zbog konveksnosti. Zaključujemo,

$$0 \neq v_1 - v_2 \in S \cap L,$$

što znači da smo konstruirali nenul točku rešetke u S. Ovime je dopunjen dokaz teorema Minkowskog uz pretpostavku da je volumen od S strogo veći od $2^n\det(L)$.

Prepostavimo sada da je S zatvoren i dozvolimo jednakost $\mathrm{Vol}(S) = 2^n\det(L)$. Za svaki $k \geq 1$ proširimo S faktorom $1 + \frac{1}{k}$ i primjenom ranijeg rezultata pronađimo nenul vektor

$$0 \neq v_k \in \left(1 + \frac{1}{k}\right)S \cap L.$$

Svaki od vektora rešetke $v_1, v_2, \ldots$ nalazi se u omeđenom skupu $2S$. Zbog diskretnosti rešetke L taj niz vektora može sadržavati samo konačno mnogo različitih vektora pa stoga možemo odabrati neki v koji se u tom nizu pojavljuje beskonačno mnogo puta. Time je pronađen nenul vektor $v \in L$ koji se nalazi u presjeku

$$\bigcap_{k=1}^{\infty}\left(1+\frac{1}{k}\right)S. \tag{13}$$

Pretpostavka zatvorenosti skupa S povlači da je navedeni presjek (13) jednak S, pa je $0 \neq v \in S \cap L$. $\square$

Dokaz Hermiteovog teorema. Ovaj dokaz je jednostavna primjena teorema Minkowskog. Neka je $L \subset \mathbb{R}^n$ rešetka te S hiperkocka u $\mathbb{R}^n$, centrirana u ishodištu tako da su joj svi bridovi duljine $2B$, odnosno

$$S = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : -B \leq x_i \leq B, \qquad \forall \quad 1 \leq i \leq n\}.$$

Skup S je simetričan, zatvoren i omeđen, a volumen mu je jednak

$$\mathrm{Vol}(S) = (2B)^n.$$

Odaberemo li $B = det(L)^{\frac{1}{n}}$, tada je $\mathrm{Vol}(S) = 2^n \det(L)$, možemo primijeniti teorem Minkowskog i zaključiti da postoji vektor $0 \neq a \in S \cap L$. Zapišemo li koordinate od a u obliku $(a_1, \ldots, a_n)$, po definiciji skupa S imamo

$$||a|| = \sqrt{a_1^2 + \cdots + a_n^2} \leq \sqrt{n}B = \sqrt{n}\det(L)^{\frac{1}{n}}.$$

Ovime je upotpunjen dokaz Teorema 24. $\square$

6 Babajev algoritam i rješavanje apprCVP pomoću "dobre" baze

Ako rešetka $L \subset \mathbb{R}^n$ ima bazu $v_1, \ldots, v_n$ koja se sastoji od vektora koji su u parovima ortogonalni, odnosno takvih da je

$$v_i \cdot v_j = 0, \qquad \forall i \neq j,$$

tada je lako riješiti i SVP (The Shortest Vector Problem) i CVP (The Closest Vector Problem). U tom slučaju, kako bismo riješili problem najkraćeg vektora (SVP), uočimo da je duljina svakog vektora u L dana formulom

$$||a_1v_1 + a_2v_2 + \cdots + a_nv_n||^2 = a_1^2||v_1||^2 + a_2^2||v_2||^2 + \cdots + a_n^2||v_n||^2.$$

Kako su $a_1, \ldots, a_n \in \mathbb{Z}$, lako je uočiti da je najkraći nenul vektor u L jednostavno najkraći vektor u skupu $\{\pm v_1, \ldots, \pm v_n\}$. Naravno, može ih biti i više najkraćih.

Slično, rješavamo li CVP, tj. želimo li pronaći najbliži vektor iz L nekom zadanom vektoru $w \in \mathbb{R}^n$, prvo ćemo zapisati

$$w = t_1v_1 + t_2v_2 + \cdots + t_nv_n, \qquad t_1, t_2, \ldots, t_n \in \mathbb{R}.$$

Zatim za $v = a_1v_1 + a_2v_2 + \cdots + a_nv_n \in L$ imamo:

$$||v - w||^2 = (a_1 - t_1)^2||v_1||^2 + (a_2 - t_2)^2||v_2||^2 + \cdots + (a_n - t_n)^2||v_n||^2. \tag{14}$$

Kako a_i moraju biti cijeli brojevi, izraz (14) se minimizira ako za svaki pojedini a_i odaberemo cijeli broj najbliži odgovarajućem realnom broju t_i.

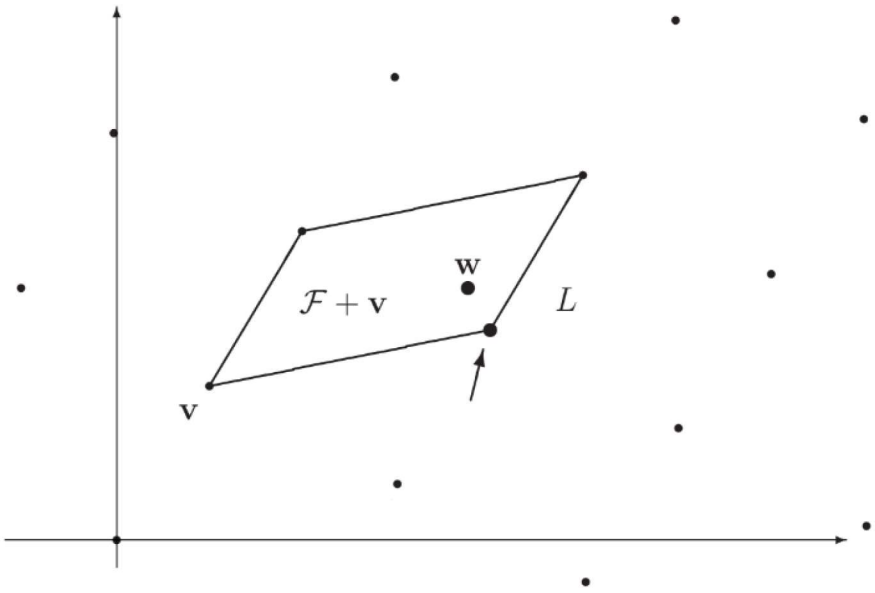
Primamljivo je pokušati provesti sličnu proceduru za proizvoljnu bazu rešetke L. Ukoliko su vektori u toj bazi približno međusobno ortogonalni, onda će rješavanje CVP vjerojatno biti uspješno. Imamo li pak bazu koja je daleko od ortogonalne, algoritam neće dobro raditi. Kratko ćemo razmotriti geometriju koja se krije iza ovakve ideje, opisati generalnu metodu te ju demonstrirati na dvodimenzionalnom primjeru.

Baza $\{v_1, \ldots, v_n\}$ za L određuje fundamentalnu domenu $\mathcal{F}$ na uobičajen način. Translatiranjem $\mathcal{F}$ elementima iz L možemo ispuniti cijeli prostor $\mathbb{R}^n$, pa je svaki $w \in \mathbb{R}^n$ dobiven jedinstvenim translatiranjem $\mathcal{F} + v$ fundamentalne domene $\mathcal{F}$ za vektor $v \in L$. Hipotetsko rješenje za CVP je vrh paralelepipeda $L + v$ koji je najbliži w. Procedura je ilustrirana na Slici 3 ([3, Figure 6.3]).

Taj najbliži vrh je lako pronaći jer je

$$w = v + \epsilon_1 v_1 + \epsilon_2 v_2 + \cdots + \epsilon_n v_n$$

za neke $0 \leq \epsilon_1, \epsilon_2, \ldots, \epsilon_n < 1$ pa jednostavno zamijenimo ϵ_i s 0 ako je manji od $\frac{1}{2}$ ili s 1 ako je veći ili jednak od $\frac{1}{2}$.



Slika 3: Korištenje zadane fundamentalne domene za rješavanje CVP

Pogledamo li Sliku 3., kandidat za (približno) najbliži vektor vektoru w je vrh paralelograma $\mathcal{F} + v$ označen strelicom. Na ovoj slici čini se da takva procedura dobro funkcionira, no to je zato što su bazni vektori na slici približno međusobno ortogonalni.

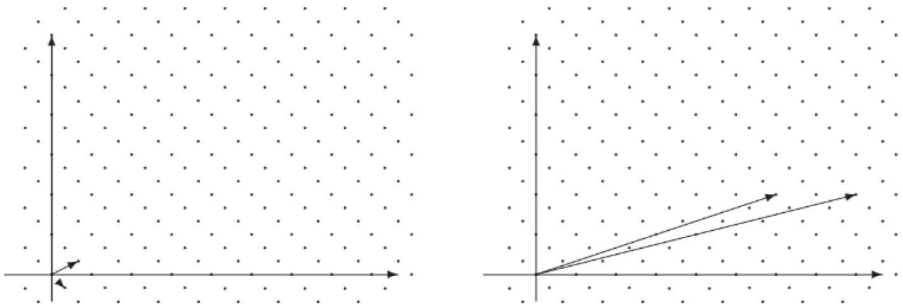
Na Slici 4 ([3, Figure 6.4]) prikazane su dvije baze za istu rešetku. Prva baza je "dobra" u smislu da su bazni vektori donekle ortogonalni, a druga "loša" jer je kut između baznih vektora poprilično mali.

Pokušamo li riješiti CVP koristeći tako lošu bazu, vjerojatno ćemo naići na problem ilustriran na Slici 5 ([3, Figure 6.5]). Naime, ciljana točka koja je izvan rešetke je ustvari poprilično blizu točki rešetke, ali je paralelogram toliko izduljen da je najbliži vrh ciljanoj točki poprilično daleko. Važno je i napomenuti da se ovakav problem još više pogoršava povećanjem dimenzije rešetke. Vizualizacija u manjim dimenzijama niti ne opisuje dovoljno do koje razine je sljedeći algoritam problematičan za rješavanje apprCVP. Zbog toga želimo da je baza poprilično ortogonalna.

Teorem 28. (Babajev algoritam za najbliži vrh) ([3, Theorem 6.34.]) *Neka je $L \subset \mathbb{R}^n$ rešetka s bazom $v_1, \ldots, v_n$ te $w \in \mathbb{R}^n$ proizvoljan vektor. Označimo s $\lfloor t_i \rceil$ najbliži cijeli broj realnom broju t_i. Ako su vektori u bazi dovoljno međusobno ortogonalni, tada sljedeći algoritam rješava CVP:*

Označimo $w = t_1 v_1 + t_2 v_2 + \cdots + t_n v_n, \qquad t_1, t_2, \ldots, t_n \in \mathbb{R}.$
Postavimo $a_i = \lfloor t_i \rceil \quad$ za $\quad i = 1, 2, \ldots, n.$
Vrati vektor $v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n.$

Općenito, ako su vektori u bazi razumno međusobno ortogonalni, tada algoritam rješava neku verziju apprCVP, no ukoliko su bazni vektori daleko od ortogonalnih, tada je vektor rezultat algoritma generalno daleko od najbližeg vektora rešetke vektoru w.



Slika 4: "Dobra" i "loša" baza za istu rešetku

Primjer 29. ([3, Example 6.35.]) Neka je $L \subset \mathbb{R}^2$ rešetka zadana bazom

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

Iskoristit ćemo Babajev algoritam (Teorem 28.) kako bismo pronašli vektor u L najbliži vektoru

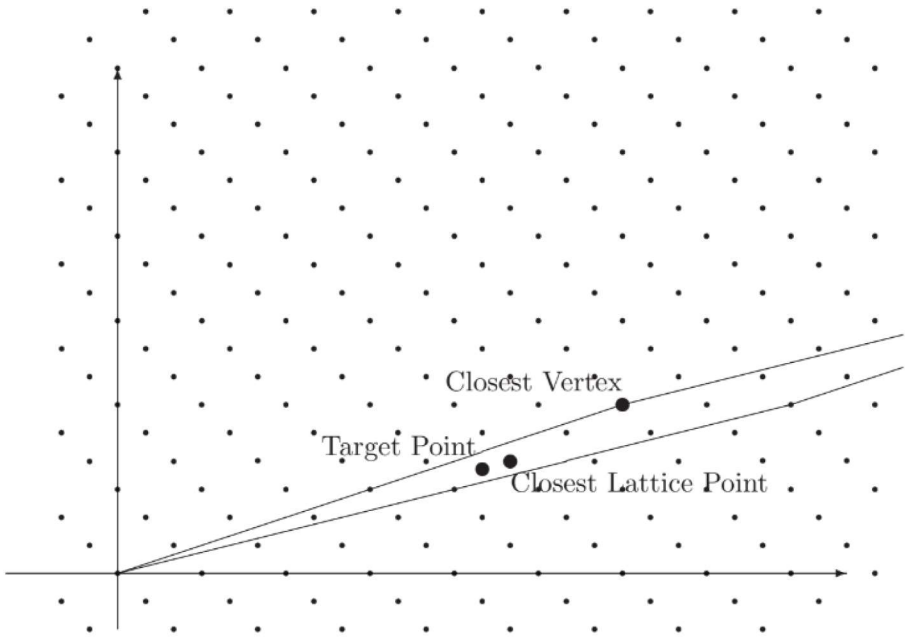
$$w = (53172, 81743).$$

Prvo treba izraziti w kao linearnu kombinaciju vektora v_1 i v_2 s realnim koeficijentima. Drugim riječima, treba pronaći $t_1, t_2 \in \mathbb{R}$ takve da vrijedi

$$w = t_1 v_1 + t_2 v_2.$$

Time dobivamo dvije linearne jednadžbe

$$53172 = 137 t_1 + 215 t_2 \qquad \text{i} \qquad 81743 = 312 t_1 - 187 t_2, \tag{15}$$



Slika 5: Babajev algoritam ne funkcionira za "lošu" bazu

ili, u matričnom zapisu,

$$(53172, 81743) = (t_1, t_2)\begin{pmatrix} 137 & 312 \\ 215 & -187 \end{pmatrix}. \tag{16}$$

Lako je odrediti (t_1, t_2) rješavanjem sustava (15) ili invertiranjem matrice u (16). Dobivamo $t_1 \approx 296.85$ i $t_2 \approx 58.15$. Babajev algoritam govori da trebamo zaokružiti t_1 i t_2 na najbliže cijele brojeve te zatim izračunati

$$v = \lfloor t_1 \rceil v_1 + \lfloor t_2 \rceil v_2 = 297(137, 312) + 58(215, -187) = (53159, 81818).$$

Dobiveni v je u L i treba biti blizu w. Dobivamo

$$||v - w|| \approx 76.12,$$

što je poprilično malo. To smo mogli i očekivati, s obzirom da su bazni vektori prilično međusobno ortogonalni. To, naime, vidimo iz činjenice da je Hadamardov omjer

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

relativno blizu 1. Pokušajmo sada riješiti isti problem najbližeg vektora koristeći istu rešetku, ali novu bazu

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

Sustav linearnih jednadžbi

$$(53172, 81743) = (t_1, t_2)\begin{pmatrix} 1975 & 438 \\ 7548 & 1627 \end{pmatrix} \tag{17}$$

ima rješenje $(t_1, t_2) \approx (5722.66, -1490.34)$, pa postavljamo

$$v' = 5723v_1' - 1490v_2' = (56405, 82444).$$

Dobiveni vektor v' je u L, ali nije baš blizu w jer je

$$||v' - w|| \approx 3308.12.$$

Neortogonalnost baze $\{v_1', v_2'\}$ može se iščitati i iz vrlo male vrijednosti Hadamardovog omjera

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

7 GGH kriptosustav s javnim ključem

Ana započinje odabirom skupa linearno nezavisnih vektora

$$v_1, v_2, \ldots, v_n \in \mathbb{Z}^n$$

koji su razumno međusobno ortogonalni. Jedan način za napraviti to je fiksirati parametar d i odabrati koordinate od $v_1, v_2, \ldots, v_n$ na slučajan način u rasponu između $-d$ i d. Ana može provjeriti je li njezin odabir vektora dobar izračunom Hadamardovog omjera za svoju bazu (Napomena 27.). Dobiveni broj ne smije biti premali. Odabrani vektori $v_1, v_2, \ldots, v_n$ su Anin tajni ključ. Radi praktičnosti, neka je V matrica veličine $n \times n$ čiji su redovi odabrani vektori $v_1, v_2, \ldots v_n$ te L rešetka generirana tim vektorima.

Ana zatim odabire $n \times n$ matricu U s cjelobrojnim koeficijentima takvu da je $\det(U) = \pm 1$. Jedan način za kreirati takvu matricu U je izmnožiti velik broj slučajno odabranih elementarnih matrica. Ana zatim računa

$$W = UV.$$

Redovi matrice W su vektori $w_1, w_2, \ldots, w_n$ koji čine novu bazu za L. Oni predstavljaju Anin javni ključ.

Želi li Ivan poslati Ani poruku, odabrat će mali vektor m kao svoj otvoreni tekst (npr. m može biti binarni vektor). Osim toga, Ivan odabire i mali perturbacijski vektor r koji ima ulogu privremenog (kratkotrajnog) ključa. Primjerice, može odabrati komponente vektora r na slučajan način u rasponu između $-\delta$ i δ, gdje je δ fiksni javni parametar. Sada treba odrediti vektor

$$e = mW + r = \sum_{i=1}^{n} m_i w_i + r,$$

koji je njegov šifrat. Uočimo da e nije točka rešetke, ali je blizu točki mW rešetke, s obzirom da je r mali vektor.

Dekripcija je vrlo jasna. Ana će iskoristiti Babajev algoritam, kako je opisano u Teoremu 29. uz dobru bazu $v_1, v_2, \ldots, v_n$ kako bi pronašla vektor u L koji je blizu vektoru e. S obzirom da koristi dobru bazu i r je mali, vektor rešetke kojeg će ona pronaći je upravo mW. Kako bi rekonstruirala otvoreni tekst m, pomnožit će inverzom W^{-1}. GGH kriptosustav sažet je u Tablici 3 ([3, Table 6.3]).

Primjer 30. ([3, Example 6.36.]) Ilustrirajmo sada GGH kriptosustav na trodimenzionalnom primjeru. Za Aninu tajnu dobru bazu uzmimo

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

Rešetka L razapeta vektorima v_1, v_2 i v_3 ima determinantu $\det(L) = 859516$, a Hadamardov omjer za tu bazu je

$$\mathcal{H}(v_1, v_2, v_3) = \left(\frac{\det(L)}{||v_1|| ||v_2|| ||v_3||} \right)^{1/3} \approx 0.7462.$$

Ana zatim množi svoju tajnu bazu matricom

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

koja ima determinantu $\det(U) = -1$, kako bi time dobila javnu bazu

$$w_1 = (-4179163, -1882253, 583183),$$
$$w_2 = (-3184353, -1434201, 444361),$$
$$w_3 = (-5277320, -2376852, 736426).$$

Hadamardov omjer za javnu bazu je vrlo mali,

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

Ivan želi Ani poslati otvoreni tekst $m = (86, -35, -32)$ uz slučajnu perturbaciju $r = (-4, -3, 2)$. Odgovarajući šifrat je

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

odnosno nakon sređivanja $e = (-79081427, -35617462, 11035473)$.

Ana za dekripciju koristi Babajev algoritam. Prvo će zapisati e kao linearnu kombinaciju vektora iz svoje tajne baze s realnim koeficijentima. Dobije se

$$e \approx 81878.97v_1 - 292300.00v_2 + 443815.04v_3.$$

Koeficijente zaokružuje na najbliže cijele brojeve i računa vektor rešetke

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

Ana	Ivan
Kreiranje ključa	
Odabire dobru bazu v_1, v_2, v_n i cjelobrojnu matricu U takvu da je $\det(U) = \pm 1$. Računa lošu bazu $w_1, w_2, \ldots, w_n$ kao redove matrice $W = UV$. Objavljuje javni ključ $w_1, w_2, \ldots, w_n$.	
Enkripcija	
	Odabire mali vektor m otvorenog teksta i slučajan mali vektor r. Koristeći Anin javni ključ, računa $e = x_1v_1 + x_2v_2 + \cdots + x_nv_n + r$. Šalje Ani šifrat e.
Dekripcija	
Koristi Babajev algoritam i računa vektor $v \in L$ najbliži vektoru e. Množi vW^{-1} i oporavlja m.	

Tablica 3: GGH kriptosustav

koji je blizu vektoru e. Zatim treba odrediti m izražavanjem vektora v u obliku linearne kombinacije javne baze i iščitati koeficijente te kombinacije. Dobiva se

$$v = 86w_1 - 35w_2 - 32w_3.$$

Pretpostavimo sada da treća osoba, Marija, želi dešifrirati Ivanovu poruku ali da zna samo javnu bazu w_1, w_2, w_3. Primijeni li Babajev algoritam, dobit će da je

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

Zaokruživanjem, dobiva vektor rešetke

$$v' = 75w_1 - 35w_2 - 24w_3 = (-79508353, -35809745, 11095049),$$

što je donekle blizu e. No, ovaj vektor rešetke vodi do pogrešnog otvorenog teksta $(76, -35, -24)$ umjesto do ispravnog $m = (86, -35, -32)$. Poučno je usporediti kako Babajev algoritam djeluje na različitim bazama. Dobivamo

$$||e - v|| \approx 5.3852 \qquad i \qquad ||e - v'|| \approx 472000.$$

Naravno, GGH kriptosustav nije siguran u dimenziji 3. Čak i ako koristimo dovoljno velike brojeve kako bismo potragu učinili iscrpljujućom i nepraktičnom, postoje učinkoviti algoritmi za pronalazak dobrih baza u manjim dimenzijama. U dvodimenzionalnom slučaju, algoritam pronalaska dobre baze potječe još od Gaussa. Vrlo moćna generalizacija za proizvoljnu dimenziju naziva se LLL algoritam i može se pronaći u [1, str. 403.-418.].

Napomena 31. GGH je primjer vjerojatnosnog kriptosustava, s obzirom da jedan otvoreni tekst može voditi do različitih šifrata, u ovisnosti o dabiru slučajne perturbacije r. Može doći do opasnosti ako Ivan šalje istu poruku dva puta koristeći različite perturbacije ili ako šalje različite poruke uz istu perturbaciju. U praksi se stoga slučajna perturbacija r određuje primjenom hash-funkcije na otvoreni tekst m.

Napomena 32. Postoji i alternativna verzija GGH kriptosustava u kojoj je zamijenjena uloga m i r. Šifrat stoga ima oblik $e = rW + m$. Ana određuje rW pronalaskom vektora rešetke najbližeg vektoru e i zatim oporavlja otvoreni tekst u u obliku $m = e - rW$.

Literatura

[1] M. Ajtai, *The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract)*, In *STOC '98: Proc. thirtieth annual ACM symposium on Theory of computing*, 10-19, ACM Press, New York, NY, 1998.

[2] O. Goldreich, D. Micciancio, S. Safra, J. P. Seifert, *Approximating shortest lattice vectors is not harder than approximating closest lattice vectors*, Inform. Process. Lett., 71(2) : 55-61, 1999.

[3] J. Hoffstein, J. Pipher, J. H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, San Francisco, CA, 2008.

[4] A. K. Lenstra, H. W. Lenstra, Jr., L. Lovasz, *Factoring Polynomials with Rational Coefficients*, Math. Ann, 261 (4): 515-534, 1982.

[5] D. Micciancio, S. Goldwasser, *Complexity of Lattice Problems*, The Kluwer International Series in Engineering and Computer Science, 671. Kluwer Academic Publishers, Boston, MA, 2002.

[6] A. M. Odlyzko, *The Rise and Fall of Knapsack Cryptosystems*, Cryptology and Computational Number Theory, volume 42 of Proc. Sympos. Appl. Math., Am. Math. Soc., Providence, RI, 1990.

Sažetak

U ovom radu bavit ćemo se teorijom rešetki i njezinim primjenama u kriptografiji. Pojam rešetke blisko je povezan s pojmom vektorskog prostora. Bavit ćemo se i temeljnim računskim problemima traženja najkraćeg (nenul) vektora u rešetci i traženjem najbližeg vektora u rešetci nekom zadanom vektoru. Pokazat će se da veliku ulogu u uspješnom rješavanju ovih problema ima ortogonalnost baze.

Ključne riječi

kongruencijski kriptosustav, problem naprtnjače, superrastući niz, Merkle-Hellman kriptosustav, rešetka, baza, ortogonalnost, fundamentalna domena, Hermiteova konstanta, Hadamardov omjer, GGH kriptosustav

Lattices and Cryptography

Summary

In this thesis, we will deal with the theory of lattices and its applications in cryptography. A lattice is similar to a vector space. The fundamental computational problems associated to a lattice are those of finding a shortest nonzero vector in the lattice and of finding a vector in the lattice that is closest to a given vector. As it shows, orthogonality of the basis plays an important role in solving these problems.

Key words

congruential cryptosystem, knapsack problem, superincreasing sequence, Merkle-Hellman cryptosystem, lattice, basis, orthogonality, fundamental domain, Hermite constant, Hadamard ratio, GGH cryptosystem

Životopis

Rođen sam 22. studenoga 1993. godine u Osijeku. Pohađao sam Osnovnu školu Miroslava Krleže u Čepinu. Nakon završetka osnovne škole, upisao sam III. gimnaziju u Osijeku (prirodoslovno-matematička gimnazija). Srednju školu sam završio 2012. godine te sam iste godine upisao preddiplomski studij matematike na Odjelu za matematiku u Osijeku. Godine 2015. završavam preddiplomski studij te upisujem diplomski studij, smjer Financijska matematika i statistika.