Razmjena ključeva prstenastim učenjem s greškama

Majcan, Borna

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

Borna Majcan

Razmjena ključeva prstenastim učenjem s greškama

Diplomski rad

Osijek, 2023.

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

Borna Majcan

Razmjena ključeva prstenastim učenjem s greškama

Diplomski rad

Mentor: izv. prof. dr. sc. Ivan Soldo

Osijek, 2023.

Sadržaj

Uvod

Potreba za zaštitom prijenosa poruka, podataka i raznih informacija iz različitih razloga javlja se još u dalekoj povijesti. U novijoj povijesti i danas potreba za sigurnom, zaštićenom i brzom komunikacijom još je bitnija jer se ljudi sve više oslanjaju na takvu komunikaciju, a i na sustave na Internetu kojima svatko može pristupiti pa je i sigurnost tih sustava također bitna.

Znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u obliku da ih samo pošaljitelj i primatelj mogu pročitati je **kriptografija**. Paralelno s kriptografijom razvija se i **kriptoanaliza**, a to je znanstvena disciplina koja se bavi proučavanjem metoda za čitanje šifriranih poruka bez poznavanja ključa.

Sigurnost kriptosustava ovisi o tajnom ključu koji pošaljitelj i primatelj trebaju razmijeniti. Ako nemaju sigurni kanal za razmjenu tajnog ključa trebaju ga razmijeniti preko nesigurnog kanala te se iz tog razloga razvijaju kriptosustavi s **javnim ključem**. Kriptosustavi s javnim ključem funkcioniraju tako da postoje javni i tajni ključ i javnim ključem se šifrira, a tajnim dešifrira polazna poruka. Tajni i javni ključ se generiraju u paru i tajni ključ uglavnom zna samo primatelj.

Prvi i još danas jako korišteni kriptosustav s javnim ključem je RSA (nazvan po autorima: Rivest-Shamir-Adleman) čija se sigurnost temelji na teškoći faktorizacije velikih prirodnih brojeva. No 1994. godine pojavljuje se **Shorov** algoritam koji je kvantni algoritam i može efikasno faktorizirati velike prirodne brojeve. Međutim još uvijek ne postoje dovoljno jaka kvantna računala da bi mogla efikasno iskoristiti Shorov algoritam. S vremenom snaga snaga kvantnih računala postaje sve veća i tehnike kojima bi mogao kriptoanalizirati RSA kriptosustav postaju sve bolje pa time smanjuju potrebnu snagu računala.

Zbog toga što trenutna kriptografija s javnim ključevima pojavom kvantnih računala više neće biti sigurna javlja se potreba za novim kriptosustavima s javnim ključem koji će biti sigurni i od napada kvanthih računala. Na taj način stvara se stvara polje post-kvantne kriptografije čiji je zadatak razviti algoritme koji će biti otporni na kriptoanalizu kvantnih računala, ali i klasičnih.

Ideja ovog rada je da se opiše jedan algoritam za koji se vjeruje da je otporan na kriptoanalizu kvantnih računala - prstenasto učenje s greškama i da se opiše protokol za razmjenu ključeva koristeći prstenasto učenje s greškama. U prvom poglavlju definiramo sve pojmove potrebne za definiciju problema od kojih su najvažniji prstenovi, rešetke, problemi rešetki - problem najkraćeg vektora, problem najbližeg

vektora i razlomački ideali. U drugom poglavlju pišemo općenito o kriptografiji, različitim generičkim kriptosustavima, spominjemo homomorfsko šifriranje i uvodimo LWE problem. U trećem poglavlju najprije navodimo neformalnu definiciju RLWE problema, a kasnije formalnu definiciju i glavni teorem redukcije koji pokazuje da se RLWE problem reducira na problem najkraćeg vektora. Naposlijetku, u četvrtom poglavlju opisujemo protokol za razmjenu ključeva koristeći RLWE.

1 Pojmovi potrebni za definiciju prstenastog učenja s greškama

U ovom poglavlju ćemo definirati sve osnovne pojmove i terminologiju potrebnu za definiranje prstenastog učenja s greškama (eng. Ring learning with errors - RLWE). RLWE temelji se na polinomima te ćemo najprije definirati prsten u kojemu su definirane dvije algebarske operacije - zbrajanje i množenje koje zadovoljavaju odgovarajuća svojstva. Sljedeće ćemo definirati prsten polinoma, konačnog polja i polja $\mathbb{F}_p$ koje ima p elemenata.

Zatim ćemo definirati pojam rešetki jer se težina RLWE problema svodi na težinu problema rešetki - problem najkraćeg vektora i problem najbližeg vektora od kojih su oba problema teška za riješiti. Drugim riječima, ne postoji efikasan algoritam, ni kvantni ni klasični, koji bi te probleme mogao riješiti u polinomnom vremenu. Još su nam potrebni razlomački ideali koji se koriste u definiciji RLWE i prsten cijelih brojeva polja K koji se koristi u glavnom teoremu redukcije.

Nadalje ćemo još dodatno definirati ciklotomske polinome te neka njihova svojstva. Ciklotomski polinomi imaju korijene koji su međusobno jednako udaljeni na jediničnoj kružnici u kompleksnoj ravnini. Ti polinomi isto imaju ulogu u definiranju RLWE. Još definiramo reducibilne (ireducibilne polinome) koji se mogu (ne mogu) faktorizirati kao umnožak dva polinoma koji imaju stupanj manji od početnog polinoma, ali veći od 0. Ti polinomi također imaju ulogu u definiranju RLWE.

Uz sve ove definicije navodimo i potrebne teoreme za dijeljenje i dobivanje ostatka pri dijeljenju polinoma jer traženje ostatka pri dijeljenju polinoma ima ključnu ulogu u RLWE.

Nakon toga moći ćemo potpuno i jasno prezentirati RLWE kriptosustav.

1.1 Algebarske strukture za RLWE

U kriptosustavu prstenastog učenja s greškama (RLWE) polinomi imaju ključnu ulogu. Kako se u kriptografiji jako često koriste ostaci cjelobrojnog dijeljenja, ovdje se koriste ostaci dijeljenja s polinomima. Da bi radili s traženim stvarima potrebno je definirati prsten polinoma i ostale algebarske strukture koje će se koristiti u radu.

1.1.1 Prsten

Prsten je skup P na kojm su definirane dvije algebarske operacije: zbrajanje $+ : P \times P \to P$ i množenje $\cdot : P \times P \to P$ sa sljedećim svojstvima:

1. $a + (b + c) = (a + b) + c, \forall a, b, c \in P$ (asocijativnost zbrajanja)

2. $\exists\ 0 \in P$, tako da $0 + a = a + 0 = a, \forall a \in P$ (neutralni element)

3. $\forall a \in P, \exists - a \in P$ tako da $a + (-a) = (-a) + a = 0$ (suprotni element)

4. $a + b = b + a, \forall a, b \in P$ (komutativnost zbrajanja)

5. $(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a, b, c \in P$ (asocijativnost množenja)

6. $a \cdot (b + c) = a \cdot b + a \cdot c$ i $(b + c) \cdot a = b \cdot a + c \cdot a$, $\forall a, b, c \in P$ (distributivnost slijeva i zdesna).

Dodatno, prsten P je **komutativan** ako vrijedi $a \cdot b = b \cdot a, \forall a, b \in P$. Prsten P je **prsten s jedinicom** ako postoji element $e \in P$ tako da $a \cdot e = e \cdot a = a, \forall a \in P$.

Neka je P komutativan prsten s jedinicom 1. Skup $P[x]$ je skup svih polinoma nad P, tj. izraza oblika $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, gdje su $a_0, \ldots, a_n \in P$. Lako se može provjeriti da je $P[x]$ komutativan prsten polinoma. Nama će od posebnog interesa biti prsten polinoma nad cijelim brojevima, tj. $\mathbb{Z}[x]$.

1.1.2 Konačno polje

U prstenastom učenju s greškama koeficijenti polinoma i sve operacije s tim koeficijentima će biti na konačnom polju. Karakteristika[1] polja po definiciji je najmanji broj puta koji se mora koristiti neutralni element za množenje (1) da se u sumi dobije neutralni element za zbrajanje (0). Ako suma nikada ne dolazi do neutralnog elementa za zbrajanje, onda prsten ima karakteristiku nula. Neka je $\mathbb{F}_q$ konačno polje s q elemenata karakteristike k. Polje $\mathbb{F}_q$ sadrži polje $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ i $\mathbb{F}_q$ je konačno-dimenzionalni vektorski prostor nad $\mathbb{F}_p$.

Polje $\mathbb{F}_p$ sastoji se od elemenata $\{0, \ldots, p-1\}$ i na njemu su definirane operacije $+$, $-$, $\cdot$ na isti način kao i u običnom polju, ali ako je rezultat izvan skupa $\{0, \ldots, p-1\}$ on se zamjeni s ostatkom cjelobrojnog dijeljenja s p.

[1] definicija karakteristike polja, ne u smislu karakteristike kao opisa/ekvivalencije

1.1.3 Rešetke (eng. lattice)

U ovom poglavlju objasnit ćemo što su to rešetke jer naš RLWE problem pripada u generičke kriptosustave temeljene na problemu rešetki.

Ugrubo govoreći, rešetka je skup točaka u n-dimenzionalnom vektorskom prostoru s periodičkom strukturom. Sada slijedi precizna definicija:

Definicija 1 (Rešetka)**.** *Za n-linearno nezavisnih vektora $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$ rešetka $\mathcal{L} \subset \mathbb{R}^n$ generirana njima je skup vektora*

$$\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\}.$$

Vektori $\mathbf{b}_1, \ldots, \mathbf{b}_n$ čine *bazu* rešetke. Rešetke mogu imati više baza, tj. baza nije jedinstvena. U sljedećoj definiciji sadržano je jedno važno svojstvo rešetke:

Definicija 2. *n-dimenzionalna rešetka $\mathcal{L}$ je diskretna aditivna podgrupa od $\mathbb{R}^n$.*

Sada opišimo značenje Definicije 2. Za početak, kako je rešetka $\mathcal{L}$ podgrupa od $\mathbb{R}^n$, to znači da $\mathcal{L}$ sadrži nul-vektor $\mathbf{0} \in \mathbb{R}^n$ i da za proizvoljni $\mathbf{x}, \mathbf{y} \in \mathcal{L}$ vrijedi $-\mathbf{x} \in \mathcal{L}$ i $\mathbf{x} + \mathbf{y} \in \mathcal{L}$. Nadalje, da je rešetka diskretna znači da za svaki $\mathbf{x} \in \mathcal{L}$ postoji neka okolina u kojoj je $\mathbf{x}$ jedini element rešetke. To se formalno zapisuje kao: $\forall \mathbf{x} \in \mathcal{L},\ \exists\, \varepsilon > 0$ tako da $(\mathbf{x} + \varepsilon\mathcal{B}) \cap \mathcal{L} = \mathbf{x}$ za $(\mathbf{x} + \varepsilon\mathcal{B})$ što predstavlja otvorenu kuglu radijusa ε s centrom u $\mathbf{x}$.

U Definiciji 1 spominjali smo bazu rešetki te sada navodimo točnu definiciju:

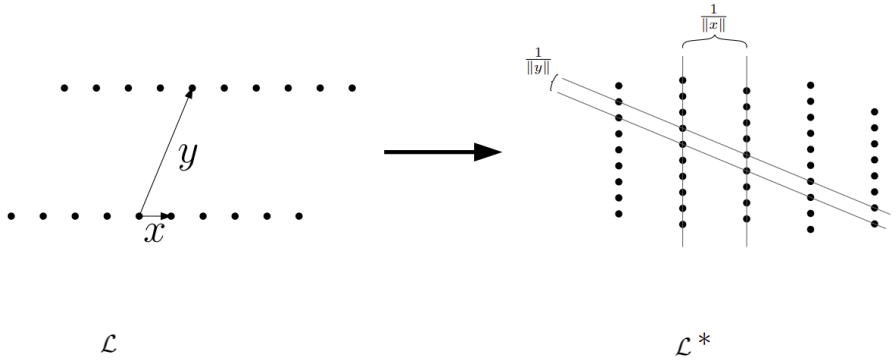
Definicija 3 (Baze rešetki)**.** *Baza $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$ rešetke $\mathcal{L}$ je skup linearno nezavisnih vektora $\mathbf{b}_1, \ldots, \mathbf{b}_n$ čije cjelobrojne linearne kombinacije razapinju rešetku:*

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

Prije nego što definiramo minimalnu udaljenost rešetke i iskažemo i dokažemo Minkowskijeve teoreme definirajmo još i dualnu rešetku:

Definicija 4 (Dualna rešetka)**.** *Neka je $\mathcal{L} \subseteq \mathbb{R}^n$ rešetka i neka je V linearna ljuska baze od $\mathcal{L}$. Dualna rešetka od $\mathcal{L}$ je skup:*

$$\mathcal{L}^* = \{\mathbf{y} \in V : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z},\ \forall \mathbf{x} \in \mathcal{L}\}.$$



Slika 1: Primjer rešetke i njenog duala [19]

Dakle, dual rešetke $\mathcal{L}$ je skup svih točaka čiji je skalarni produkt s bilo kojim elementom rešetke cijeli broj. U Definiciji 4 izraz $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ interpretira se tako da ako je rezultat skalarnog produkta cijeli broj, onda to svojstvo vrijedi. Također, nekada se za dualnu rešetku s elementima u $\mathbb{R}^n$ kaže da je to $\mathbb{Z}$-dual [4]. Postoji još jedna definicija dulane rešetke, ali s elementima u nekom polju $\mathbb{K}$ stupnja n. Za tu definiciju treba nam pojam trag polja, a za trag polja su potrebni pojmovi podpolja, proširenja polja i polje proširenja.

Trag polja

U ovom dijelu želimo doći do definicije traga polja koja će biti potrebna u definiciji RLWE. Počnimo s pojmom podpolja. Podskup $\mathbb{K}$ polja $\mathbb{F}$, $\mathbb{K} \subseteq \mathbb{F}$ je **podpolje** polja $\mathbb{F}$ ako je $\mathbb{K}$ polje uz sve naslijeđene operacije iz $\mathbb{F}$. Nadalje, ako je $\mathbb{K}$ podpolje od $\mathbb{F}$, onda je $\mathbb{F}$ **proširenje polja** $\mathbb{K}$; dodatno $\mathbb{F}$ je **konačno proširenje** polja $\mathbb{K}$ ako je $\mathbb{F}$ konačno-dimenzionalni vektorski prostor nad $\mathbb{K}$. Oznaka za dimenziju od $\mathbb{K}$ je $[\mathbb{F} : \mathbb{K}]$. Za kraj, par ta dva polja, $\mathbb{F}$ i $\mathbb{K}$, takva da su operacije iz $\mathbb{F}$ naslijeđene u $\mathbb{K}$ je **polje proširenja** te se označava s $\mathbb{F}/\mathbb{K}$. Jedan primjer polja proširenja je polje realnih brojeva $\mathbb{R}$ nad poljem kompleksnih brojeva $\mathbb{C}$, tj. $\mathbb{C}/\mathbb{R}$.

Do sada smo koristili samo pojam polja, ali za nastavak trebamo definirati i pojam **polja brojeva** što se definira kao polje proširenja $\mathbb{K} = \mathbb{Q}(\zeta)$, dobiveno spajanjem apstraktnoga elementa ζ i polja racionalnih brojeva, gdje ζ zadovoljava uvjet $f(\zeta) = 0$, za neki ireducibilni polinom $f(x) \in \mathbb{Q}[x]$ (više o ireducibilnim polinomima u Poglavlju 1.3 i Definiciji 20). Specijalno, polje $\mathbb{Q}(\zeta_n)$ je **ciklotomsko polje** n-tih korijena iz jedinica, za $\zeta_n = e^{\frac{2\pi i}{n}}$. Još za polinom f bez smanjenja općenitosti možemo napraviti da mu je vodeći koeficijent jednak jedan jer u suprotnom polinom

f možemo podijeliti s vodećim koeficijentom te $f(\zeta) = 0$ ostaje vrijediti, a ni ostali korijeni polinoma se dijeljenjem ne mijenjaju. Polinom f je **minimalni polinom** od ζ i stupanj polja brojeva isti je kao i stupanj polinoma f. Kako je $f(\zeta) = 0$ po pretpostavci, onda se na polje brojeva $\mathbb{K}$ može gledati kao vektorski prostor nad poljem $\mathbb{Q}$ s bazom $\{1, \zeta, \ldots, \zeta^{n-1}\}$ koja se zove **baza potencija** od $\mathbb{K}$.

Nadalje, neka imamo dva vektorska prostora $\mathbf{V}$ i $\mathbf{W}$ nad istim poljem $\mathbb{F}$. Funkcija $f : \mathbf{V} \to \mathbf{W}$ je **linearno preslikavanje** ako je za sve elemente $\mathbf{v}, \mathbf{w} \in \mathbf{V}$, $\lambda \in \mathbb{F}$ zadovoljena **homogenost** i **aditivnost**, tj. $f(\lambda\mathbf{v}) = \lambda f(\mathbf{v})$ i $f(\mathbf{v} + \mathbf{w}) = f(\mathbf{v}) + f(\mathbf{w})$.

Neka je sada $\mathbb{K}$ polje i $\mathbb{F}$ konačno proširenje ($\mathbb{K} \subseteq \mathbb{F}$, $\mathbb{F}/\mathbb{K}$). Za proizvoljni $\lambda \in \mathbb{K}$ definirajmo množenje s λ kao linearno preslikavanje $m_\lambda : \mathbf{V} \to \mathbf{V}$ s pravilom pridruživanja $m_\lambda(\mathbf{v}) = \lambda\mathbf{v}$. Uz tako definirano linearno preslikavanje $m_\lambda(\mathbf{v})$, **trag polja** $tr_{\mathbb{K}/\mathbb{F}}(\lambda) : \mathbb{K} \to \mathbb{F}$ definiran je kao običan trag u linearnoj algebri od ovog linearnog preslikavanja. Ovo je općenita definicija, ali za nas će proširenje biti skup racionalnih brojeva $\mathbb{Q}$.

Još želimo iskazati trag polja koristeći korijene minimalnoga polinoma pa se sada malo vratimo i na minimalni polinom od m_λ nad $\mathbb{K}$ i na njegove korijene. Neka su $\sigma_1(\lambda), \ldots, \sigma_n(\lambda) : \mathbb{K} \to \mathbb{C}$ korijeni minimalnoga polinoma. Trag polja je definiran s:

$$tr = tr_{\mathbb{K}/\mathbb{Q}}(\lambda) = \sum_{i=1}^{n} \sigma_i(\lambda).$$

Trag je aditivan i multiplikativan.

Sada smo objasnili i definirali sve pojmove potrebne za definiciju dualne rešetke u polju, što će biti potrebno za definiciju RLWE problema.

Definicija 5. *Neka je $\mathcal{L}$ rešetka u polju $\mathbb{K}$ stupnja n. Njezin dual je:*

$$\mathcal{L}^\vee = \left\{\alpha \in \mathbb{K} : tr_{K/\mathbb{Q}}(\alpha\mathcal{L}) \subset \mathbb{Z}\right\}.$$

Uz problem rešetki još se vežu i problem najbližeg vektora i problem najkraćeg vektora. Za njih je potrebno znanje i minimalne udaljenosti rešetke.

Definicija 6. *Minimalna udaljenost rešetke $\mathcal{L}$ je:*

$$\lambda_1(\mathcal{L}) := \min_{\mathbf{v} \in \mathcal{L} \setminus \{\mathbf{0}\}} ||\mathbf{v}|| = \min_{\mathbf{x} \neq \mathbf{y} \in \mathcal{L}} ||\mathbf{x} - \mathbf{y}||. \tag{1}$$

Jedan bitan rezultat u kriptografiji temeljenoj na rešetkama je Minkowskijev teorem koji daje gornju među za minimalnu udaljenost rešetke. Sada navodimo taj teorem i jedanu njegovu posljedicu.

Teorem 1 (Minkowskijev teorem, vidjeti [16, Teorem 2.14]). *Bilo koje konveksno centralno simetrično tijelo S volumena takvog da $vol(S) > 2^n \cdot det(\mathcal{L})$ sadrži ne-nula element rešetke.*

Prije dokaza napomenimo da je tijelo S centralno simetrično ako vrijedi $\mathbf{x} \in S \iff -\mathbf{x} \in S$ i da je S konveksan ako $\forall \mathbf{x}, \mathbf{y} \in S \Rightarrow \lambda\mathbf{x} + (1-\lambda)\mathbf{y} \in S,\ \forall \lambda \in [0,1]$. Dodatno, skup $\mathcal{F} \subset \mathbb{R}^n$ je fundamentalno područje rešetke $\mathcal{L}$ ako svi $\mathbf{x} + \mathcal{F} = \{\mathbf{x} + \mathbf{y} : \mathbf{y} \in \mathcal{F}\}$, $\forall \mathbf{x} \in \mathcal{L}$ čine particiju od $\mathbb{R}^n$.

Dokaz. Najprije definirajmo $S_2 = \frac{S}{2}$ tako da $\text{vol}(S_2) > \det(\mathcal{L})$. Sada želimo pokazati da postoje $\mathbf{a}, \mathbf{b} \in S_2$, $\mathbf{a} \neq \mathbf{b}$ tako da $\mathbf{a}, \mathbf{b} \in \mathcal{L}$. Zato uzmimo fundamentalno područje $\mathcal{F}$ od $\mathcal{L}$ i particionirajmo sve S_2 u skupove $S_\mathbf{s} = S_2 \cap (\mathbf{s} + \mathcal{F}),\ \forall \mathbf{s} \in \mathcal{F}$. Tada translatirana područja takva da $S_\mathbf{s} - \mathbf{s} \subseteq \mathcal{F}$ imaju ukupni volumen $\text{vol}(S_2) > \text{vol}(\mathcal{F})$ što znači da se preklapaju na nekom području. Dakle, $\exists \mathbf{k} \in (S_\mathbf{c} - \mathbf{c}) \cap (S_\mathbf{d} - \mathbf{d})$ za $\mathbf{c} \neq \mathbf{d} \in \mathcal{L}$ te se tako dobiva da su $\mathbf{a} = \mathbf{k} + \mathbf{c},\ \mathbf{b} = \mathbf{k} + \mathbf{d}$ različite točke u S_2 i razlika im je $\mathbf{a} - \mathbf{b} = \mathbf{c} - \mathbf{d} \in \mathcal{L}$, što je element rešetke. Još uzmimo $2\mathbf{a}, -2\mathbf{b} \in S$ pa po definiciji centralne simetrije S_2 i zbog konveksnosti vrijedi $\frac{2\mathbf{a}-2\mathbf{b}}{2} = \mathbf{x} - \mathbf{y} \in S$. To smo i željeli pokazati. □

Korolar 1 (Minkowskijev prvi teorem, vidjeti [16, Korolar 2.15]). *Za proizvoljnu rešetku $\mathcal{L}$ vrijedi:*

$$\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot \det(\mathcal{L})^{\frac{1}{n}}. \tag{2}$$

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti da $\det(\mathcal{L}) = 1$ jer svaku bazu možemo skalirati da to dobijemo i to trebamo skalirati skalarom $\det(\mathcal{L})^{-\frac{1}{n}}$. Međutim, skaliranjem baze također se i λ_1 skalira za isti skalar. Nadalje, imamo $S = \sqrt{n}\mathcal{K}$ što je zatvorena kugla u l_2 normi radijusa $\sqrt{n}$. Primijetimo da kocka $[-1,1]^n$ ima duljinu stranica 2 pa i volumen 2^n i sadržana je u kugli S te slijedi da je $vol(S) > 2^n$. Sada su zadovoljeni uvjeti Minkowskijevog teorema 1. Slijedi da S sadržava ne-nula element rešetke pa je $S = \sqrt{n}\mathcal{K}$ i gornja međa λ_1 je omeđena $\lambda_1 \leq \sqrt{n}$. To smo i željeli pokazati. □

Sada kako smo naveli sve potrebno za definiciju najbližeg i najkraćeg vektora i Minkowskijev prvi teorem čiji će rezultat biti koristan u određivanju gornje međe tih problema.

Problem najkraćeg vektora (eng. Shortest Vector Problem; ubuduće: SVP)

To je jednostavno problem pronalaska duljine (oznaka: $\lambda_1(\mathcal{L})$) najkraćeg nenula vektora u $\mathcal{L}$. Problem se može definirati na bilo kojoj normi, ali je najčešća l_2 norma. Minkowskijevim teoremom pokazano je da je problem odozgo omeđen s $\sqrt{n} \cdot \det(\mathcal{L})^{\frac{1}{n}}$. Sada imamo preciznu definiciju:

Definicija 7 (Problem najkraćeg vektora)**.** *Problem SVP-a ima sljedeće tri varijante gdje se kao baza rešetki bez smanjenja općenitosti koriste samo vektori s cjelobrojnim koeficijentima:*

1. *Odluka: uz poznavanje baze* $\mathbf{B} \in \mathbb{Z}^{m \times n}$ *i* $d > 0 \in \mathbb{R}$*, razlikovati slučajeve* $\lambda_1(\mathcal{L}(\mathbf{B})) \leq d$ *i* $\lambda_1(\mathcal{L}(\mathbf{B})) > d$*.*

2. *Računanje: uz poznavanje baze* $\mathbf{B}$ *pronaći* $\lambda_1(\mathcal{L}(\mathbf{B}))$*.*

3. *Pretraga: uz poznavanje baze* $\mathbf{B}$ *pronaći* $\mathbf{v} \in \mathcal{L}(B)$*,* $v \neq 0$ *tako da* $||v|| = \lambda_1(\mathcal{L}(\mathbf{B}))$*.*

Sve tri varijante su ekvivalentne. Još jedna bitna varijanta SVP problema je aproksimacijski SVP:

Definicija 8 (Aproksimacijski SVP)**.** γ*-aproksimacijski SPV, za* $\gamma = \gamma(n) \geq 1$ *što je funkcija koja ovisi o dimenziji rešetke* n*, ima sljedeće tri varijante:*

1. *Odluka (*$GapSVP_\gamma$*): uz poznavanje baze* $\mathbf{B} \in \mathbb{Z}^{m \times n}$ *i* $d > 0 \in \mathbb{Z}$*, razlikovati slučajeve* $\lambda_1(\mathcal{L}(\mathbf{B})) \leq d$ *i* $\lambda_1(\mathcal{L}(\mathbf{B})) > d \cdot \gamma$*.*

2. *Procjena (eng. Estimation) (*$EstSVP_\gamma$*): uz poznavanje baze* $\mathbf{B}$*, izračunati* $\lambda_1(\mathcal{L}(\mathbf{B}))$ *do* γ *faktora, tj. izračunati neke* $d \in [\lambda_1(\mathcal{L}(\mathbf{B}), \gamma \cdot \lambda_1(\mathcal{L}(\mathbf{B}))]$ *.*

3. *Pretraga (*SVP_γ*): uz poznavanje baze* $\mathbf{B}$*, pronaći* $\mathbf{v} \in \mathcal{L}(B)$*,* $v \neq 0$ *tako da* $0 < ||v|| \leq \gamma \cdot \lambda_1(\mathcal{L}(\mathbf{B}))$*.*

Primijetimo da se za $\gamma = 1$ u sve tri varijante dobiva ista verzija problema. Osim toga, problem postaje lakši kako γ postaje veći. Za razliku od SVP-a gdje su sva tri problema ekvivalentna, u aproksimacijskom SVP-u vrijedi $GapSVP_\gamma \leq EstSVP_\gamma \leq SVP_\gamma$. To znači, ako je moguće riješiti Pretraga varijantu, onda je moguće riješiti Procjena varijantu, a to na kraju znači da je moguće riješiti Odluka varijatnu.

Problem najbližeg vektora (eng. Closest Vector Problem; ubuduće: CVP)

To je jednostavno problem pronalaska elementa rešetke koja je najbliža traženoj točki t (koja nije nužno element rešetke). Problem se može definirati na bilo kojoj normi, ali najčešća je l_2 norma. Imamo sljedeću definiciju:

Definicija 9 (Problem najbližeg vektora)**.** *Za dani aproksimacijski element/faktor $\gamma = \gamma(n) \geq 1$ imamo tri varijante:*

1. *Odluka: uz poznavanje $\mathbf{B} \in \mathbb{Z}^{m \times n}$ baze rešetke, $\mathbf{t} \in \mathbb{Z}^m$, $r \in \mathbb{Q}$, razlikovati slučajeve $dist(\mathbf{t}, \mathcal{L}(\mathbf{B})) \leq r$ i $dist(\mathbf{t}, \mathcal{L}(\mathbf{B})) \leq \gamma r$.*

2. *Procjena: uz poznavanje baze $\mathbf{B} \in \mathbb{Z}^{m \times n}$ i vektora $\mathbf{t}$, pronaći $d > 0$ tako da $dist(\mathbf{t}, \mathcal{L}(\mathbf{B})) \in [d, \gamma d]$.*

3. *Pretraga: uz poznavanje baze $\mathbf{B} \in \mathbb{Z}^{m \times n}$ i vektora $\mathbf{t} \in \mathbb{Z}^m$, pronaći $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ tako da $||\mathbf{v} - \mathbf{t}|| \leq \gamma \cdot dist(\mathbf{t}, \mathcal{L}(\mathbf{B}))$.*

1.1.4 Ideali

Cilj ovog poglavlja je opisati što je $R^\vee = t^{-1}R$, a to će se pojaviti u definiciji i primjeru RLWE.

Definicija 10 (Lijevi i desni ideal)**.** *Za proizvoljni prsten $(R, +, \cdot)$ neka je $(R, +)$ aditivna grupa.*

Lijevi ideal: *Podskup I je lijevi ideal u prstenu R ako vrijedi sljedeće:*

1. *$(I, +)$ je podgrupa od $(R, +)$,*

2. *$\forall a \in I, b \in R$ vrijedi $ba \in I$.*

Primijetimo da to znači: podskup I je lijevi ideal u prstenu R ako je on aditivna podgrupa koja apsorbira množenje slijeva od elemenata iz R.

Desni ideal: *Za desni ideal vrijedi sve analogno osim drugog svojstva koje glasi:*

2. *$\forall a \in I, b \in R$ vrijedi $ab \in I$.*

Definicija 11 (Ideal)**.** *Ako je I lijevi i desni ideal u prstenu R, onda je I obostrani ideal u R ili samo ideal u R.*

Razlomački i dualni ideal

U radu će nam biti potrebni razlomački (eng. fractional) i dualni ideali. Za početak krenimo s R-modulom, što je jednostavno vektorski prostor nad prstenom R pa navedimo formalnu definiciju:

Definicija 12 (R-modul)**.** *Neka je R komutativni prsten. R-modul je aditivna abelova grupa M s definiranim skalarnim množenjem $\cdot : R \times M \to M$ tako da za $m, n \in M$ i $p, q, 1 \in R$ vrijede aksiomi:*

1. $p \cdot (m + n) = p \cdot m + p \cdot n$,

2. $(p + q) \cdot m = p \cdot m + q \cdot m$,

3. $(p \cdot q) \cdot m = p \cdot (q \cdot m)$,

4. $1 \cdot m = m$.

Napomena 1. *Primijetimo da je R-modul definiran na način iz prethodne Definicije 12 vektorski prostor nad prstenom R jer je aditivna grupa. To znači da zadovoljava prva četiri aksioma vektorskog prostora i zatvoren je na zbrajanje. Nadalje, kako je $R \times M \to M$ zatvoreno na množenje skalarom iz R i četiri nabrojana aksioma su četiri aksioma vektorskih prostora. Tako smo obrazložili zašto je R-modul vektorski prostor nad prstenom R.*

Sada nastavimo s definiranjem podmodula. Podmodul P je R-modul koji je sadržan u većem R-modulu M tako da ako $p_1, p_2 \in P$ i $r \in R$, onda $p_1 + p_2$ i rp_1 imaju isto značenje u P kao i u M. Navedimo formalnu definiciju:

Definicija 13 (Podmodul)**.** *Neka je M R-modul. Podmodul N od M je aditivna podgrupa N od M zatvorena za skalarno množenje (ako je $n \in N$ i $r \in R$, onda $rn \in N$).*

Definicija 14 (Razlomačko polje)**.** *Neka je polje $\mathbb{F}$ konstruirano iz R na način da je R domena i polje $\mathbb{F}$ sadrži R kao podprsten te neka za svaki $f \in \mathbb{F}$ postoje $a, b \in R$, $b \neq 0$ tako da $f = ab^{-1}$. Tako konstruirano polje $\mathbb{F}$ je razlomačko polje i označava se s $Frac(R)$.*

Jedan očiti primjer razlomačkog polja od $\mathbb{Z}$ je $\mathbb{Q}$ i pišemo $Frac(\mathbb{Z}) = \mathbb{Q}$.

Još nam za definiciju razlomačkog ideala preostaje definirati konačno generiran modul.

Definicija 15 (Konačno generiran modul)**.** *Modul M je konačno generiran ako je M konačno generiran nekim konačnim skupom. Drugim riječima, ako postoji konačan podskup $X = \{x_1, \ldots, x_n\}$ s*

$$M = \langle X \rangle = \left\{ \sum_i r_i x_i : r_i \in \mathbb{R}, x_i \in X \right\}.$$

Definicija 16 (Razlomački ideal)**.** *Neka je R domena te neka vrijedi $F = Frac(R)$. Razlomački ideal je konačno generiran ne-nula R-podmodul od F, ako je I ne-nula ideal u R i vrijedi $I^{-1} = \{v \in F : vI \subseteq R\}$.*

Uvijek vrijedi da $I^{-1}I \subseteq R$. Razlomački ideal je invertibilan ako vrijedi $I^{-1}I = R$. Ako je I razlomački ideal, onda je $I^V = I^{-1}R^V$ njegov **dualni ideal**.

1.1.5 Prsten cijelih brojeva polja K

Definicija 17 (Integral nad prstenom)**.** *Neka je R podprsten komutativnog prstena S. Element $x \in S$ je integral nad R ako postoji jedinični polinom f u $R[x]$ takav da $f(x) = 0$.*

Definicija 18 (Integralno zatvorenje (eng. integral closure))**.** *Neka je R podprsten komutativnog prstena S tako da $1 = 1_S \in R$. Integralno zatvarnaje od R u S je skup elemenata od S koji su integrali nad R.*

Definicija 19 (Prsten cijelih brojeva polja K)**.** *Neka je K polje brojeva. Prsten cijelih brojeva u K je integralno zatvorenje od $\mathbb{Z}$ u K i označava se s $\mathcal{O}_K$.*

1.2 Dijeljenje polinoma

U daljnjem dijelu ovog rada susretat ćemo se sa situacijama gdje ćemo trebati dijeliti polinome, ali još više i dobivanjem ostatka pri dijeljenju polinoma. Kako bi bili sigurni u ispravnost ovog procesa oslanjamo se na teorem o dijeljenju s ostatkom koji jamči da su pri dijeljenju dva polinoma kvocijent i ostatak jedinstveni polinomi.

Dodatno, kako bi dokazali teorem o dijeljenju s ostatkom trebat će nam još i teorem o nul-polinomu. On tvrdi da je polinom nul-polinom ako i samo ako su mu svi koeficijenti jednaki nula.

Teorem 2 (o nulpolinomu, vidjeti [15, Teorem 1])**.** *Polinom $f(x) = a_0 + a_1 x + \cdots + a_n x^n, a_i \in \mathbb{R}$, $\forall i = 0, \ldots, n$ je nulpolinom $(f(x) = 0, \forall x \in \mathbb{R}) \iff$ vrijedi $a_0 = \cdots = a_n = 0$.*

Dokaz. $\boxed{\Leftarrow}$ Za $a_i = 0, \forall i = 0, \ldots, n$ jasno je da je $f(x)$ nulpolinom ($f(x) = 0, \forall x \in \mathbb{R}$).
$\boxed{\Rightarrow}$ $f(x) = 0, \forall x \in \mathbb{R}$. Pretpostavimo suprotno, tj. da nisu svi elementi jednaki 0 te da postoji $m \geq 0$ tako da $p = n - m$ i $a_0 = \cdots = a_{m-1} = 0$, $a_m \neq 0$. Nadalje definirajmo novi $p := n - m$ i $b_0 := a_m, b_1 := a_{m+1}, \ldots, b_p := a_{m+p} (= a_n)$. Primijetimo da je $p = n - m \iff n = p + m$.
Sada imamo nove koeficijente za $f(x)$ koji su po pretpostavci različiti od 0 za $m \geq 0$. Možemo zapisati $f(x)$ pomoću novih koeficijenata koristeći samo one koji su različiti od 0. Još po pretpostavci smjera znamo kako je $f(x)$ nulpolinom pa izjednačavanjem s nulom dobivamo:

$$f(x) = b_0 x^m + b_1 x^{m+1} + \cdots + b_p x^{m+p} = 0 \ / : x^m \neq 0$$

$$b_0 + b_1 x + \cdots + b_p x^p = 0, \forall x \in \mathbb{R} \setminus \{0\}.$$

Također imamo:

$$-b_0 = b_1 x + \cdots + b_p x^p \ / \ |\cdot|$$
$$|b_0| = |b_1 x + \cdots + b_p x^p|.$$

Sada definirajmo novi $M := \max\{|b_1|, \ldots, |b_p|\} > 0$. Uzmimo $x \in \left\langle 0, \frac{1}{2} \right\rangle$. Imamo:

$$\begin{aligned} |b_0| &= |b_1 x + \cdots + b_p x^p| \leq |b_1| x + \cdots + |b_p| x^p \\ &\leq Mx \left(1 + x + \cdots + x^{p-1}\right) \leq Mx \left(1 + \tfrac{1}{2} + \tfrac{1}{2^2} + \cdots + \tfrac{1}{2^{p-1}}\right) \\ &= Mx \underbrace{\frac{1 - \frac{1}{2^p}}{1 - \frac{1}{2}}}_{2(1 - \frac{1}{2^p})} = 2Mx - \underbrace{\frac{1}{2^{p-1}} Mx}_{\geq 0} \leq 2Mx. \end{aligned}$$

$\Rightarrow \frac{|b_0|}{2M} \leq x, x \in \left\langle 0, \frac{1}{2} \right\rangle$. Uvrstimo za $x = \frac{1}{3}, \frac{1}{4}, \ldots, \frac{1}{k}, \ldots$ i slijedi da je $b_0 = 0$ što je kontradikcija s pretpostavkom $b_0 = a_m \neq 0$. Dobivamo da je pretpostavka bila kriva i da onda nužno vrijedi $a_0 = \cdots = a_n = 0$. To smo i željeli pokazati. □

Teorem 3 (o dijeljenju s ostatkom, vidjeti [15, Teorem 3])**.** *Za svaka dva polinoma $f, g \in \mathbb{R}[x]$, $g \neq 0$ postoje jedinstveni polinomi $q, r \in \mathbb{R}[x]$ tako da vrijedi:*

$$f = g \cdot q + r.$$

Ako je $r \neq 0$, vrijedi $st\ r < st\ g$.

Dokaz. Najprije pokažimo *jedinstvenost*: Pretpostavimo suprotno, tj. za dane f i g $\exists q, r$ i q', r' tako da je $q \neq q'$ i $r \neq r'$.

$$f = g \cdot q + r$$
$$f = g \cdot q' + r'.$$

Oduzimanjem dobivamo

$$0 = g \underbrace{(q - q')}_{\neq 0} + \underbrace{(r - r')}_{\neq 0}.$$

Sada poznavanjem Teorema 2 o nulpolinomu dobivamo kontradikciju.

Sada dokažimo *egzistenciju*. Razdvojimo na dva slučaja: 1) st $f <$ st g i 2) st $f \leq$ st g. Za prvi slučaj 1) st $f <$ st g jednakost mogu zadovoljiti polinomi $q = 0$ i $r = f$. Za drugi slučaj 2) st $f \geq$ st g. Za početak imamo polinome f i g:

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$
$$g(x) = b_m x^m + \cdots + b_1 x + b_0.$$

Sada definirajmo novi polinom f_1 na način:

$$f_1(x) := f(x) - \frac{a_n}{b_m} x^{n-m} g(x). \tag{3}$$

Označimo $n_1 :=$ st f_1. Još raspišimo f_1 da potvrdimo kako smo konstruirali f_1 na način da je $n_1 < n$. Imamo:

$$\begin{aligned} f_1(x) &= a_n x^n + \cdots + a_0 - \frac{a_n}{b_m} x^{n-m}(b_m x^m + \cdots + b_0) \\ &= \cancel{a_n x^n} + \cdots + a_0 - \cancel{a_n x^n} - \frac{a_n b_{m-1}}{b_m} x^{n-1} + \cdots . \end{aligned}$$

Sada se vidi da je $n_1 < n$ i još napišimo f_1 u kanonskom obliku:

$$f_1(x) = c_{n_1}^{(1)} x^{n_1} + \cdots + c_0^{(1)}.$$

Ako je $n_1 \geq m$ postupak nastavljamo i definiramo $f_2(x)$ analogno kao i $f_1(x)$; analogno jednadžbi (3) imamo:

$$f_2(x) := f_1(x) - \frac{a_n}{b_m} x^{n-m} g(x). \tag{4}$$

Sada imamo $n_2 =$ st f_2 te analogno formiramo kanonski zapis od f_2 i nastaviti definirati nove polinome $f_3, f_4, \ldots$ te oni čine padajući niz po stupnju polinoma i

nastaviti se sve dok se ne vrijedi st $f_k < m$ ili $f_k(x) = 0$. Još napišimo za k-ti polinom za koji vrijedi prethodna tvrdnja:

$$f_k(x) := f_{k-1}(x) - \frac{c_{n_2}^{(k-1)}}{b_m} x^{n_{k-1}-m} g(x). \tag{5}$$

Sada zbrojimo sve novo formirane f_k-ove (3), (4), ..., (5). Odmah je vidljivo da se prekriženi elementi poništavaju i imamo:

$$\begin{aligned}
\cancel{f_1(x)} &= f(x) - \frac{a_n}{b_m} x^{n-m} g(x) \\
\cancel{f_2(x)} &= \cancel{f_1(x)} - \frac{c_{n_1}^{(1)}}{b_m} x^{n_1-m} g(x) \\
&\vdots \\
f_k(x) &= \cancel{f_{k-1}(x)} - \frac{c_{n_2}^{(k-1)}}{b_m} x^{n_{k-1}-m} g(x).
\end{aligned}$$

Za ukupni zbroj dobivamo:

$$\underbrace{f_k(x)}_{=:r(x)} = f(x) \underbrace{-\left(\frac{a_n}{b_m} x^{n-m} + \frac{c_{n_1}^{(1)}}{b_m} x^{n_1-m} + \cdots + \frac{c_{n_{k-1}}^{(k-1)}}{b_m} x^{n_{k_{n-1}}-m}\right)}_{=:q(x)} g(x),$$

$$f(x) = q(x) \cdot g(x) + r(x), \text{ st } r < \text{st } g.$$

To smo i željeli pokazati.

□

Primjer 1 (dijeljenja polinoma)**.** *Odrediti ostatak $r(x)$ pri dijeljenju polinoma $f(x) = -x^6 + 5x^5 - 4x^4 + 3x^3 - x^2 + 5x - 4$ s polinomom $g(x) = x^4 + 1$.*

Dobivamo:

$$\begin{array}{rrl}
-x^6 + 5x^5 - 4x^4 + 3x^3 - x^2 + 5x - 4 = \left(x^4 + 1\right)\left(-x^2 + 5x - 4\right) + 3x^3 & & \\
\hline
x^6 \qquad\qquad\qquad + x^2 & & \\
\hline
5x^5 - 4x^4 + 3x^3 & + 5x & \\
-5x^5 \qquad\qquad\quad - 5x & & \\
\hline
-4x^4 + 3x^3 & - 4 & \\
4x^4 \qquad\qquad + 4 & & \\
\hline
3x^3 & &
\end{array}$$

Sada smo polinom f napisali u obliku $f(x) = q(x) \cdot g(x) + r(x)$, gdje je nepotpuni kvocijent $q(x) = -x^2 + 5x - 4$ i ostatak $r(x) = 3x^3$.

1.3 Specifični polinomi

U ovom poglavlju najprije definiramo reducibilne, ireducibilne polinome koji su bitni u definiciji RLWE. Sljedeće definiramo ciklotomske polinome; polinomi čiji korijeni na jediničnoj kružnici u kompleksnoj mreži su međusobno jednako udaljeni te oni su isto bitni za definiciju RLWE, ali i za kriptografiju općenito jer su u tom području često korišteni.

Nadalje navodimo jednu značajnu lemu o ciklotomskim polinomima za proste n čiji će se rezultat koristiti kasnije u ovom radu. Da bi dokazali tu lemu navodimo dvije leme koje će se koristiti u dokazu: jednu lemu s laganim dokazom indukcijom, a drugu lemu kojoj preskačemo dokaz jer on zahtijeva znanje iz kompleksne analize što izlazi iz opsega ovog rada.

Definicija 20 (Reducibilni polinom)**.** *Neka je $\mathbb{F}$ polje. Ne-konstantni polinom f je reducibilan nad $\mathbb{F}$ ako se može faktorizirati kao produkt polinoma g i $h \in \mathbb{F}[x]$ gdje su stupnjevi od g i h manji od stupnja f; odnosno:*

$$f = g \cdot h,$$

$$st(g), st(h) < st(f).$$

Ne-konstantni polinom $f(x)$ je ireducibilan nad $\mathbb{F}$ ako nije reducibilan. Tako npr. za $f(x) = x^4+3$ vrijedi da je reducibilan nad $\mathbb{R}$ jer $x^4+3 = (x^2-\sqrt{3})(x^2+\sqrt{3})$, a nije reducibilan nad $\mathbb{Q}$.

Definicija 21 (n-ti ciklotomski polinom)**.** *Za proizvoljni pozitivni cijeli broj n, n-ti ciklotomski polinom je jedinstveni ireducibilan polinom s cjelobrojnim koeficijentima koji je djelitelj od $x^n - 1$ i nije djelitelj od $x^k - 1$, za svaki $k < n$.*

Navedimo alternativnu definiciju ciklotomskih polinoma koristeći umnoška polinoma koja će za dokaze biti korisnija:

Definicija 22 (n-ti ciklotomski polinom)**.** *Za proizvoljni pozitivni cijeli broj n, n-ti ciklotomski polinom dan je formulom:*

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ gcd(k,n)=1}} (x - e^{2i\pi\frac{k}{n}}).$$

Podsjetimo se da je izraz e^{ix} definiran s:

$$e^{ix} = cos(x) + isin(x).$$

Primijetimo da je stupanj polinoma Φ_n jednak $\varphi(n)$, gdje je φ Eulerova funkcija. Više o Eulerovoj funkciji i njenim svojstvima se može naći u [8]. Još pokažimo jednu nama značajnu karakteristiku o ciklotomskim polinomima, ali najprije iskažimo dvije leme potrebne za dokaz.

Lema 1. *Za proizvoljan $n \in \mathbb{N}$ vrijedi:*

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1 = \sum_{k=0}^{n-1} x^k.$$

Dokaz. Dokaz provodimo matematičkom indukcijom.
Baza $n = 1$: $\frac{x-1}{x-1} = 1$;
Pretpostavka: neka formula vrijedi za proizvoljan $n \in \mathbb{N}$, tj.
$\frac{x^n-1}{x-1} = x^{n-1} + x^{n-2} + \cdots + x + 1$;
Korak: Pokažimo da vrijedi i za $n + 1$:

$$\frac{x^{n+1} - 1}{x - 1} = \frac{x^{n+1} - x^n + x^n - 1}{x - 1} = \frac{x^n(x-1) + (x^n - 1)}{x - 1}$$
$$= x^n + \frac{x^n - 1}{x - 1} = x^n + x^{n-1} + \cdots + x + 1.$$

To smo i željeli pokazati. □

Lema 2 (vidjeti [1, Lema 6])**.** *Za proizvoljni $n \in \mathbb{N}$ vrijedi:*

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Dokaz ove leme nije jednostavan i može se naći u [1, Lema 6]. Dakle, sada imamo sve leme potrebne za dokaz značajne leme o ciklotomskim polinomima za proste n.

Lema 3 (O ciklotomskim polinomima za proste n)**.** *Neka je n prost broj. Vrijedi:*

$$\Phi_n(x) = 1 + x + x^2 + \cdots + x^{n-1} = \sum_{k=0}^{n-1} x^k.$$

Dokaz. Za početak imamo $\Phi_1(x) = x - 1$. Koristeći Lemu 2 imamo $x^n - 1 = \Phi_n(x)\Phi_1(x)$ i još dodatno $\Phi_n(x) = \frac{x^n-1}{\Phi_1(x)} = \frac{x^n-1}{x-1}$. Sada koristeći Lemu 1 imamo $\sum_{k=0}^{n-1} x^k$. To smo i željeli pokazati. □

2 Općenito o post-kvantnoj sigurnosti, vrstama ključeva i o prstenastom učenju s greškama

Glavni razlog zašto se bavimo prstenastim učenjem s greškama (skraćeno: RLWE - ring learning with errors) je taj što želimo konstruirati kriptografski sustav koji će biti siguran od kriptoanalize kvantnih računala. RLWE pruža sigurnosna jamstva za koje se vjeruje[2],[3] da se ne mogu probiti trenutno poznatim algoritmima na kvantnim računalima te je to dobar kandidat za kriptosustav koji će biti siguran od kriptoanalize kvantnih računala.

2.1 Generički kriptosustavi koji su kandidati za post kvantnu sigurnost

Generički kriptosustavi su skupine kriptosustava koji se temelje na istoj matematičkoj ideji i svoju sigurnost temelje na istome. Neki primjeri generičkih kriptosustava za koje se vjeruje da su trenutno poznatim algoritmima sigurni od kriptoanalize kvantnih računala dijele se u šest različitih generičkih skupina:

◇ Kriptografija bazirana na rešetkama: tu pripadaju učenje s greškama, prstenasto učenje s greškama, NTRU, itd.. Sigurnost ove skupine kriptsustava temelji se na pretpostavci da je problem rešetki težak problem (npr. problem najkraćeg vektora). Ti kriptosustavi u svojoj konstrukciji koriste rešetke ili ih koriste samo u dokazu sigurnosti.

◇ Multivarijatna kriptografija: tu pripadaju neuravnotežena shema ulja i octa (eng. Unbalanced Oil and Vinegar Signature Schemes[12]), duga (eng. Rainbow) (zajedno sa SIDH-om (2.1) nije više siguran kriptosustav[2]), itd.. Ova skupina kriptosustava koristi se s polinomima više varijabli nad konačnim poljem $\mathbb{F}$ i sigurnost temelji se na činjenici da je rješavanje sustava multivarijabilnih polinoma NP-potpun[10].

◇ Kriptografija bazirana na hash funkcijama: tu pripadaju Merklova shema potpisa

[2]Ovdje i u ostatku ovog rada će se u kontekstu sigurnosti od kvantnih računala govoriti 'vjeruje' iz dva razloga: zato što su kvantna računala još uvijek u ranoj fazi razvoja i zato što je moguće da će se otkriti novi algoritam (sličan shorovom) koji će moći vršiti kriptoanalizu.

[3]To vjeruju Oded Regev i Daniele Micciancio (matematičar i informatičar koji živi u SAD-u) u članku [14], a Chris Peikert ide i korak dalje te tvrdi da su to vodeći kandidati za post kvantnu sigurnost[17].

(eng. Merkle Signature Scheme), Lamportov potpis (eng. Lamport signature), itd.. Ova skupina kriptosustava temelji se na sigurnosti hash funkcija.

◇ Kriptografija temeljena na kodu (eng. Code-based cryptography): tu pripada McElice kriptosustav. Ova skupina kriptosustava temelji se na kodovima koji ispravljaju pogreške. To je tehnika koja se koristi za ispravljanje pogreški u prijenosu podataka preko loših kanala (npr. radio prijenos podataka od udaljenih odašiljača ili bilo kakvih odašiljača od kojih se dobiva loš signal); ta tehnika nije povezana s kriptografijom, ali može se koristiti u tom području.

◇ Kvantno otporni simetrični ključ: tu pripadaju AES i SNOW 3G. Ovo je jedina generička skupina u nabrojanima koja koristi simetrični ključ i kao takva je brža i efikasnija, ali ne nudi opciju da pošaljitelj i primatelj razmjene ključ preko nesigurnog kanala. Više o razlici simetričnih i asimetričnih ključeva reći ćemo u poglavlju 2.2.

∗ Kriptografija temeljena na izogenijama supersingularnih eliptičkih krivulja (SIDH). Taj kriptosustav[4] je isto bio obećavajući kandidat za zaštitu od kriptoanalize kvantnih računala, ali je 2022. godine u radu [3] otkrivena učinkovita kriptoanaliza i to čak ne teoretska kao npr. Shorovim algoritmom preko kvantnih računala, nego baš praktična na klasičnim računalima. Više o ovoj temi i događaju se može vidjeti u web novinskom članku [11].

2.2 Vrste ključeva

Osnovna podjela kriptosustava po vrsti ključa je: simetrični ključ (poznata još kao: tajni ključ) i na asimetrični ključ (poznata još kao: javni ključ).

Kriptosustavi sa simetričnim ključem

Kriptosustav je simetričan ako se poznavanjem ključa za šifriranje (dešifriranje) može lagano izračunati ključ za dešifriranje (šifriranje), no često su to i isti ključevi. Generalno dobra stvar oko tih kriptosustava je to što je na taj način puno lakše napraviti siguran kriptosustav koji će biti efikasan, brz, a i težak za kriptoanalizu klasičnim i kvantnim računalima; doduše problem je što se za sigurnost zahtijeva da pošaljitelj i primatelj imaju siguran kanal preko kojega će taj ključ razmijeniti. Npr. veoma poznata enigma je imala tu vrstu ključa pa su se za komunikaciju preko

[4] nije generički kriptosustav kao ostali na listi, nego je "obični" kriptosustav

enigme koristili predefinirani ključevi za određeno vrijeme unaprijed i svaki ključ je vrijedio za jedan dan.


Geheime Kommandosache! Jede einzelne Tagesschlüssel ist geheim. Mitnahme im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

Monats-tag	Walzenlage	Ringstellung	an der Umkehrwalze	Steckerverbindungen am Steckerbrett 1 2 3 4 5 6 7 8 9 10	Kenngruppen
649 31	I V III	14 09 24		SZ GT DV KU FO MY EW JN IX LQ	wny dgy ekb rzg
649 30	IV III II	05 26 02		IS EV MX RW DT UZ JQ AO CH NY	ktl acw zsi wao
649 29	III II I	12 24 03	KM AX PZ GO	DJ AT CV IO ER QS LW PZ FN BH	ioc zcn ovw wvd
649 28	II III V	06 08 16	DI CN BR PV	CR FV AI DK OT MQ EU BX LP GJ	lrb cld ude rzh
649 27	III I IV	11 03 07	LT EQ HS UW	DY IN BV GR AM LO FP HT EX UW	woj fbh vct uis
649 26	I IV V	17 22 19		VZ AL RT KO CG EI BJ DU FS HP	xle gbo uev rxm
				OB FV AD IT PK HJ LZ NS EQ CW	ouc uhq uew uit

Slika 2: Ključevi za enigmu [7]

Svakako enigma nije jedini kriptosustav sa tajnim ključem. Postoje i suvremeni kriptosustavi koji koriste tajni ključ; primjeri: Blowfish, ChaCha20, AES (Advanced Encryption Standard) koji je najčešći kriptosustav koji koristi simetrični ključ te je danas jako upotrebljivan u svijetu. Ti sustavi ipak su generalno bolji za dugoročnu komunikaciju između dvije strane (možda nije najbolje rečeno, ali komunikaciju na veliko ili slično).

Kriptosustavi s asimetričnim ključem

Kriptosustav je asimetričan ako ima dva ključa, javni i tajni, koji su matematički povezani, ali to na način da poznavanjem javnog ključa se poruka šifrira, a tajnim ključem se dešifrira. Poznavanjem javnog ključa ne može se lagano pronaći tajni ključ. Ti sustavi pošiljatelju i primatelju omogućuju da mogu sigurno razmijeniti tajni ključ i ako nemaju sigurni kanal komunikacije. S obzirom kako ti sustavi imaju javni i tajni ključ koji su povezani, teže je napraviti siguran sustav te je njihova sigurnost njih ipak nešto lošija od kriptosustava sa simetričnim ključem. Primjer nekih kriptosustava s asimetričnim ključem je prstenasto učenje s greškama, učenje s greškama, RSA, NTRU.

Zbog prednosti i mana jedne i druge strane, često se u praksi za komunikaciju koristi kriptosustav sa simetričnim ključem, ali se tajni ključ simetričnog sustava razmjeni preko asimetričnog sustava. Naime, kako je i opisano, simetrični sustavi su sigurniji za komunikaciju, ali je preko asimetričnog ipak potrebno razmijeniti ključ.

2.3 Homomorfsko šifriranje

Homomorfsko šifriranje je oblik šifriranja koji omogućuje da se operacije provode nad šifratom bez da ga se dešifrira. Njegovi su rezultati u šifriranom obliku isti onima koji bi se dobili da su se provodili nad ne-šifriranim podacima.

Potreba za homomorfskim šifriranjem javlja se u slučaju kada korisnik želi da netko drugi napravi neku operaciju nad podacima, ali ne želi odati svoje podatke.

Opišimo sada kako se provodi homomorfsko šifriranje provodi. Recimo da Alice želi da joj oblak obradi podatke, ali ne želi otkriti svoje podatke oblaku. Formalno, ako Alice ima podatke x i želi da joj oblak izračuna $f(x)$, taj postupak nastavlja se tako da Alice šalje šifriranu poruku $Enc(x)$ i funkciju f oblaku; zatim oblak odabire funkciju F tako da $Dec(F(Enc(x)) = f(x)$ i nazad Alicei šalje $F(Enc(x))$; za kraj, Alice dešifrira poruku i dobiva $f(x)$.

Postoji više razina homomorfskog šifriranja. Najjača razina je potpuno homomorfsko šifriranje koje omogućuje da se na šifratu provode proizvoljne operacije i proizvoljan broj operacija. Najslabija razina homomorfskog šifriranja je djelomično homomorfsko šifriranje koje omogućuje da se na šifratu provodi samo jedan tip operacija (npr. zbrajanje ili množenje).

Zanimljivo je da su kriptosustavi temeljeni na rešetkama, a posebno LWE/RLWE jedini kriptosustavi za koje je trenutno poznato kako na njima napraviti potpuno homomorfsko šifriranje.

2.4 Povijest prstenastog učenja s greškama

Prstenasto učenje s greškama (eng. Ring learning with errors - RLWE) je u kriptografiji novi pojam i pojavljuje se 2010. godine (vidjeti [13]) kao nadogradnja na Učenje s greškama (eng. Learning with errors - LWE) koje se pojavljuje 2005. godine kao rad Oded Regeva[5] (vidjeti [18]).

Prstenasto učenje s greškama (LWE) pokazalo se kao veoma raznoliko: može se koristiti kao kriptosustav s asimetričnim ključem za zaštitu od poznavanja šifrata i poznavanja otvorenog teksta, kao protokol za razmjenu ključeva i kao kriptosustav s asimetričnim ključem, kao potpuno homomorfsko šifriranje i kroz još raznih drugih korisnih stvari. Međutim, problem LWE-a je ipak to što često nije dovoljno efikasan u praksi jer su ključevi i šifrati jako veliki. Njihovu veličinu jasnije ćemo prikazati u Poglavlju 2.4.1 i Primjerima 2, 3. Javni ključ je velik jer je potrebno predati n

[5] izraelsko-američki matematičar i informatičar

vektora $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathbb{Z}_q^n$, što dovodi do ključeva reda veličine n^2 te je iz praktične perspektive poželjno smanjiti red veličine ključa na veličinu blisku linearnoj.

2.4.1 Primjer LWE

Kako je LWE prethodnik od RLWE-a zanimljivo bi nam bilo napraviti primjere šifriranja i dešifriranja LWE-om kao kriptosustavom s javnim ključem i primjer protokola za razmjenu ključeva. Provedimo dva različita načina šifriranja i jedan način protokola za razmjenu ključeva. U Primjeru 2 ukratko ćemo upisati jedan način šifriranja poruke koristeći LWE bez dijeljenja ključeva.

Primjer 2. *Najprije definirajmo poruku koju želimo poslati iz skupa $M \in \{0, 1\}$. Zatim definirajmo niz n nasumičnih vrijednosti uniformnom distribucijom $\mathcal{U}(0, N)$, $N \in \mathbb{N}$ i tako generiramo $A = \{a_1, \ldots, a_n\}$ uz kojeg ćemo generirati javni ključ. Zatim odabiremo tajni ključ $s \in \mathbb{N} \setminus \{5\}$, s neparan. Da bismo još mogli generirati drugi tajni ključ koji nam je potreban trebamo generirati grešku $e \in \mathbb{N}$, gdje je e mali broj. Uz poznavanje javnog ključa A, tajnog ključa s i greške e generiramo drugi javni ključ $B = A \cdot s + e = \{b_1, \ldots, b_n\}$. Sada kako imamo naš glavni tajni ključ B iz njega uzorkujemo elemente na proizvoljan način i generiramo $B_{uzorkovan} = B_u = \{b_{u_1}, \ldots, b_{u_m}\}$, $m \leq n$. Nakon uzorkovanja možemo generirati šifrat P na način: $P = M + \sum_{i=0}^{m} b_i$. Dešifriranje poruke radi se tako da šifrat P podijelimo s tajnim ključem s te ako je ostatak dijeljenja 0, poruka M je 0, a ako je ostatak 1, poruka M je 1.*

Na Primjeru 2 jasno se vidi da je LWE asimetrični kriptografski sustav jer smo javnim ključem B šifrirali poruku, a tajnim ključem s dešifrirali poruku. Iako javni i tajni ključ jesu povezani i to precizno formulom $B = A \cdot s + e$, uz poznavanje javnog ključa B nije lagano doznati tajni ključ s. Dokaze i dodatna objašnjenja za LWE izostavljamo jer LWE nije glavna tema, nego jedan zanimljiv primjer.

Također, primijetimo da smo u Primjeru 2 kao poruku imali samo jedan bit. Tom metodom šalje se samo jedan bit, što i je jedan od razloga zašto su šifrati i ključevi za tu metodu veliki. U Primjeru 3 pokazana je razmjena ključeva LWE-om koristeći malo drugačiju metodu od prethodnog primjera.

Primjer 3. *Analogno kao u Primjeru 2 definirajmo $M \in \{0, 1\}$ i A, tajni ključ $s \in \mathbb{N}$ te vektor greške $\mathbf{e} \in \mathbb{N}^n$ s malim vrijednostima. Dodatno je potreban prosti broj q. Generiramo javni ključ B, takav da je $B_i = A_i \cdot s + e_i \ (mod\ q)$. Sada*

imamo naše javne ključeve A i B te koristeći isključivo njih šifriramo našu poruku generirajući $u = \sum_{A_{uzorci}} A_i \ (mod\ q)$ i $v = \frac{q}{2}M + \sum_{B_{uzorci}} B_i$. Sada je šifrat (u, v). Za dešifriranje se koristi formula $D = v - su \ (mod\ q)$ te ako je D manji od $\frac{q}{2}$, onda je $M = 0$, ako je D veći od $\frac{q}{2}$, onda je $M = 1$.

Valja napomenuti da metoda objašnjena u Primjeru 3 ne radi točno u svim slučajevima, nego je samo jako vjerojatna da radi dobro. Npr. na mojim testnim podacima dolazilo je do krive razmjene ključeva u otprilike 1 od 150 slučajeva. To definitivno nije idealno i to još k tome što šaljemo bitove, ali na što većim brojevima vjerojatnost za grešku je manja. Više o tom problemu reći ćemo u RLWE dijelu.

Navedimo još primjer protokola za razmjenu ključeva:

Primjer 4. *Za primjer protokola koristit ćemo dvoje ljudi: Alice i Boba. Za početak, na proizvoljan način generiramo $A \in \mathbb{Z}_q^{n \times n}$ uniformnom distribucijom. Zatim definiramo distribuciju greške kao Gaussovu distribuciju s očekivanjem 0 i malom standardnom devijacijom (predlaže se $1.4 \leq \sigma \leq 2.8 \ll \sqrt{n}$). Alice generira svoj $r \in \mathbb{Z}^n$ distribucijom greške a Bob generira svoj $s \in \mathbb{Z}^n$ tom istom distribucijom. Zatim Alice stvara $u^T = r^T A + e_a$ (e_a je vektor greške iz distribucije greške), ubuduće označeno kao $u^T \approx r^T A$ i Bob analogno stvara $v \approx As$. Alice računa $r^T v \approx r^T As \approx k$ a Bob računa $k \approx u^T s \approx u^T As$. Sada oboje imaju sličnu vrijednost k. Bob želi Alice poslati jedan bit M i to radi na način da šalje $c = k + M \cdot \frac{q}{2}$. Alice dešifrirava c tako da gleda je li $c \approx k$. Ako je blizu, onda je poslani bit 0, inače 1. Sada više bitova nije sigurno slati uz iste A, r, s, no nije potrebno generirati sve nove, nego je dovoljno generirati samo jedan novi r ili s ili oboje te nije potrebno generirati novi A.*

2.4.2 Ideja za učenje s greškama nad prstenima

Ranije smo spomenuli kako su ključevi za LWE veliki i potrebno je n^2 operacija modulo q za šifrirati i dešifrirati poruku. Da bismo dobili jedan skalar $b_i \in \mathbb{Z}_q$ koji je naizgled nasumičan, potreban je red veličine n operacija modulo q jer množimo nasumični vektor redak $a_i \in \mathbb{Z}^{1 \times n}$ s tajnim vektorom $s \in \mathbb{Z}^n$: $a_i \cdot s + e_i = b_i \in \mathbb{Z}_q$. Javni ključ $A \in \mathbb{Z}^{n \times n}$ i $b \in \mathbb{Z}_q^n$ također su reda veličina n^2 pa se postavljalo pitanje kako smanjiti veličinu ključa i broja operacija za šifriranje i dešifriranje poruka.

Dakle, bio je problem kako napraviti neku drugačiju operaciju od množenja vektora na opisani način: $a_i \star s_i + e_i = b_i$, ali tako da još uvijek proizvodimo b_i na naizgled nasumičan način. Primjerice, množenje vektora pa koordinatama ne

bi proizvodilo vektore b_i na naizgled nasumičan način i to bi bio lagan problem za riješiti. Jedno rješenje bilo je promatrati vektor a_i i vektor s kao polinome i vršiti polinomno množenje između ta dva vektora u polinomnom prstenu $\mathbb{Z}_q/(X^n + 1)$. Tako bi javni ključ A postao element $\mathbb{Z}_q^n$ i smanjila bi se veličina ključeva na $\mathbb{Z}_q^n$ te bi za stvaranje vektora b, $A \star s + e = b \in \mathbb{Z}_q^n$ bilo potrebno $n\log n$ operacija modulo q.

3 Prstenasto učenje s greškama

3.1 Uvod

Najprije navedimo neke pojmove i izraze koji se često spominju u RLWE-u.

Neka je $f(x) = x^n + 1 \in \mathbb{Z}[x]$, gdje je n potencija broja 2 te je na taj način $f(x)$ ireducibilan polinom nad poljem $\mathbb{R}$. Neka je $R = \mathbb{Z}[x]/\langle f(x)\rangle$ prsten polinoma s cjelobrojnim koeficijentima modulo $f(x)$. Dodatno, neka je $q = 1 \bmod 2n$ dovoljno veliki javni prosti modul i neka je $R_q = R/\langle q\rangle = \mathbb{Z}_q[x]/\langle f(x)\rangle$ prsten cjelobrojnih polinoma modulo $f(x)$ i q, ponekad označeno s $\bmod(f(x), q)$. Više o traženju ostatka pri dijeljenju polinoma u Poglavlju 1.2 i u Primjeru 1.

Podsjetimo se velike O notacije. Time se opisuje asimptotsko ponašanje funkcija te ugrubo, govori se koliko brzo funkcija raste. Za formalnu definiciju, neka imamo $f, g : \mathbb{R} \to \mathbb{R}$. Tada vrijedi $f(x) = O(g(x))$, za $x \to \infty$, ako postoje konstante C, N takve da $|f(x)| \leq C|g(x)|$, za sve $x > N$. Nadalje, želimo opisati i $\tilde{O}$ notaciju. $\tilde{O}$ ignorira logaritamske faktore, tj. vrijedi $O(h(n)\log^k n) = \tilde{O}(h(n)))$.

Nadalje, želimo još opisati ω notaciju. Neka imamo proizvoljnu funkciju f. Tada $\omega(f)$ označava neku proizvoljnu funkciju koja raste asimptotski brže od f, tj. $f : \mathbb{N} \to \mathbb{R}$ pripada u $\omega(g)$ za $g : \mathbb{N} \to \mathbb{R}$ (označeno kao $f = \omega(g)$) ako za svaki $k > 0$ postoji $n_0 > 0$ takav da za svaki $n \geq n_0$ vrijedi $|f(n)| \geq k\,|g(n)|$.

Oznaka $poly(n)$ označava proizvoljan polinom te $f(n) = poly(n)$ možemo interpretirati kao da postoji polinom $p(n)$ tako da je $f(n) \leq p(x)$. Funkcija $\mu : \mathbb{N} \to \mathbb{R}$ je zanemariva ako za svaki pozitivni polinom p postoji N takav da za svaki $n > N$ vrijedi $\mu(n) < \frac{1}{p(n)}$. Funkcija $f : \mathbb{N} \to \mathbb{R}$ je ogromna (eng. overwhelming) ako je $1 - f$ zanemariva funkcija.

Ovdje započnimo s neformalnom definicijom prstenastog učenja s greškama, a u idućem Poglavlju 3.2 navest ćemo i potpunu formalnu tehničku definiciju.

RLWE problem ima dvije varijante: Pretrage i Odluke. Navedimo sada neformalne definicije obje varijante:

Definicija 23 (neformalna definicija varijante odluke)**.** *Neka imamo prosti broj q. RLWE problem u R: fiksirati određenu distribuciju greške nad R koja je koncentrirana nad malim vrijednostima po apsolutnoj vrijednosti nad cijelim brojevima. Neka je $s = s(x) \in R_q$ uniformo nasumična. Cilj je raspoznati proizvoljno mnogo nezavisnih šumovitih prstenastih jednadžbi od pravih uniformnih parova. Točnije, šumovite jednadžbe su oblika $(a, b \approx a \cdot b) \in R_q \times R_q$, gdje je svaki a uniformno nasumičan, a*

svaki produkt $a \cdot s$ je perturbiran izrazom dobivenim nezavisno iz distribucije greške iz R.

Definicija 24 (neformalna definicija varijante pretrage)**.** *RLWE problem: cilj je pronaći tajni ključ $s(x)$ uz dani nasumični skup polinoma polinom $a_i(x) \in R_q$ i javnog ključa $b_i = a_i \cdot s + e_i \in R_q$, odnosno $(a_i(x), b_i(x))$, za $i = 1, \ldots, n$, $n \in \mathbb{N}$.*

Napomena 2. *U Definiciji 23 naveli smo neformalnu definiciju RLWE-problema gdje je $s = s(x) \in R_q$ izabran iz uniformne distribucije, ali se u nekim drugim radovima predlaže da je $s = s(x) \in R_q$ iz diskretne Gaussove distribucije s očekivanjem 0 i standardnom devijacijom σ gdje je σ također mali broj [9].*

Napomena 3. *U Definiciji 23 naveli smo da je $f(x) = x^n + 1$, gdje je n potencija broja 2. Također postoji još jedan pristup toj definiciji, takav da je $f(x)$ proizvoljni ciklotomski polinom [6].*

Primijetimo da u varijanti pretrage gdje imamo formulu $b_i = a_i \cdot s + e_i$ i poznate $(a_i(x), b_i(x))$ bez dodane greške e_i, da ona ne postoji ovaj problem bi bio veoma lagan za riješiti, no uz dodane greške problem više nije lagan.

Ubuduće, oznaka $\leftarrow$ će označavati da element odabran iz navedene distribucije. Napravimo sada jedan manji primjer problema prstenastog učenja s greškama:

Primjer 5. *Najprije odabiremo $a \in \mathcal{O}/q\mathcal{O}$ iz uniformne distribucije, $s, e \leftarrow \psi$ iz distribucije greške i konstruiramo $(a, b) = (a, a \cdot s + e)$ (za $\mathcal{O}$ najčešće uzimamo $\mathcal{O} = \mathbb{Z}[x]/f(x)$). Zatim definiramo poruku m kojoj su elementi bitovi i promatramo ju kao polinom $u \in \mathcal{O}/q\mathcal{O}$. Dodatno, definiramo $r, e_1, e_2 \leftarrow \psi$ i konstruiramo $u := ar + e_1$, $v := br + e_2 + \left\lfloor \frac{q}{2} \right\rfloor m$. Tako smo napravili šifrat (u, v). Sada trebamo dešifrirati šifrat uz poznavanje tajnog ključa s. To radimo tako da računamo $v - us = er + e_2 - e_1 s + \left\lfloor \frac{q}{2} \right\rfloor m$. Svaki koeficijent zaokružiti na 0 ili $\left\lfloor \frac{q}{2} \right\rfloor$, koji je bliži mod q.*

Iz ovoga primjera vidimo da je RLWE već efikasniji u šifriranju od LWE jer otvoreni tekst koji želimo šifrirati nije samo jedan bit, nego niz bitova dimenzije n.

Pojasnimo još što znači zaokružiti na 0 ili $\left\lfloor \frac{q}{2} \right\rfloor$, koji je bliži modulo q za npr. $q = 17$. Imamo koeficijente: $0, 1, 2, 3, 13, 14, 15, 16$ koji su bliži 0 mod 17 i imamo koeficijente $5, 6, 7, 8, 9, 10, 11$ koji su bliži $\left\lfloor \frac{q}{2} \right\rfloor = 8$ mod 17. Imamo i koeficijente 4 i 12 koji su jednako udaljeni 0 mod 17 i 8 mod 17 te se za njih primjenjuje pristup korišten u signal fukncijama 30, koje će se kasnije opisati u Poglavlju 4.2.

3.2 Formalna definicija RLWE

Definicija 25 (Distribucija RLWE)**.** *Za $s \in R_q^\vee$ i distribuciju greške ψ nad $K_\mathbb{R}$ uzorak iz RLWE distribucije $A_{s,\psi}$ nad $R_q \times \mathbb{T}$ ($\mathbb{T} = K_\mathbb{R}/R^\vee$) generira se odabirom $a \leftarrow R_q$ uniformno i odabirom $e \leftarrow \psi$ te izlazom $(a, b) = (a \cdot s)/q + e \bmod R^\vee$.*

RLWE kao i LWE ima dvije varijante, varijantu pretrage i varijantu odluke te njih sada definiramo:

Definicija 26 (RLWE, varijanta pretrage)**.** *Neka je ψ familija distribucija nad $K_\mathbb{R}$. Varijanta pretrage s oznakom $RLWE_{q,\Psi}$ je definirana s: uz poznavanje proizvoljno mnogo nezavisnih uzoraka iz $A_{s,\psi}$ za proizvoljan $s \in R_q^\vee$ i $\psi \in \Psi$, pronaći s.*

Varijanta pretrage: pronaći tajni element $s \in R_q^\vee$ uz poznavanje proizvoljno mnogo nezavisnih uzoraka.

$$\begin{aligned} &a_1 \leftarrow R_q, && b_1 = a_1 \cdot s + e_1 \in R_q^\vee && \\ &a_2 \leftarrow R_q, && b_2 = a_2 \cdot s + e_2 \in R_q^\vee && (e_i \leftarrow \psi) \\ & && \vdots && \end{aligned}$$

Primijetimo da problem pretrage RLWE bez dodanih grešaka, za razliku od problema pretrage LWE, nije toliko očit za riješiti. Da bi se taj problem riješio mogli bismo polinom a staviti u njegovu matričnu formu i pomnožiti vektor b inverzom matrice a, samo što taj inverz mora postojati. Međutim, a će biti invertibilan s velikom vjerojatnošću, a i ako nije, mogu se linearno zavisni vektori izbaciti i dodati jedan uzorak da se dobiju linearno nezavisni vektori.

Definicija 27 (RLWE, varijanta odluke)**.** *Neka je Υ distribucija nad familijom distribucija greški, svaka nad $K_\mathbb{R}$. Varijanta odluke RLWE problema, označena $RDLWE_{q,\Upsilon}$ (eng. ring-decision learning with errors) je raspoznati između proizvoljno mnogo nezavisnih uzoraka iz $A_{s,\psi}$ za nasumičan odabir $(s, \psi) \leftarrow U(R_q^\vee) \times \Upsilon$ i istog broja uniformno nasumičnih i nezavisnih uzoraka iz $R_q \times \mathbb{T}$.*

Varijanta odluke: raspoznati (a_i, b_i) od uniformnog $(a_i, b_i) \in R_q \times R_q^\vee$. Još je definiran i $R^\vee = t^{-1}R$.

3.3 Redukcija i rešetke

Ranije smo definirali rešetke i probleme koji su vezani za rešetke. Naveli smo da LWE i RLWE problemi pripadaju u kriptosustave temeljene na rešetkama, no u definiciji nismo koristili rešetke. Zapravo, razlog zašto za te kriptosustave smatramo da su temeljeni na rešetkama je to što se njihovi problemi mogu reducirati na probleme temeljene na rešetkama (SVP, aproksimacijski SVP, CVP) za koje je poznato da su teški problemi.

Definicija 28 (redukcija)**.** *Problem A prihvaća redukciju do problema B ako se svaka instanca A može transformirati na instancu B u polinomnom vremenu, tj. ako je rješenje B dovoljno za rješavanje A s istom razinom složenosti. Oznaka* $A \leq B$.

RLWE definiran nad dualnim $R^\vee = t^{-1}R$ sa dovoljno širokim greškama je težak, tj. vrijedi:

$$\text{najgori slučaj aproksimacijskog SVP-a na idealnim rešetkama u } R \leq \text{pretraga RLWE} \leq \text{odluka RLWE}.$$

Sada, uz ovu tvrdnju znamo da problem najgoreg slučaja aproksimacijskog SVP-a na idealnim rešetkama u R možemo reducirati do pretrage RLWE i odluke RLWE.

Prije glavnog teorema trebamo još definirati dvije distribucije ($\Psi_{\leq\alpha}$) korištene u glavnom teoremu, ali i pojašnjenje neprekidne Gaussove vjerojatnosne distribucije D_r širine r kao i prostora H.

Najprije definiramo prostor $H \subseteq \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ za $s_1 + 2s_2 = n$ definiramo kao $H = \{(x_1, \ldots, x_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} : x_{s_1+s_2+j} = \overline{x_{s_1+j}}, \forall j \in [s_2]\} \subseteq \mathbb{C}^n$. Za $r > 0$ definiramo Gaussovu funkciju $\rho_r : H \to \langle 0, 1]\,,\ \rho_r = \exp \frac{-\pi||\mathbf{x}||_2^2}{r^2}$. Normiranjem ove funkcije dobiva se neprekidna Gaussova vjerojatnosna distribucija D_r širine r s gustoćom $r^{-n}\rho_r(\mathbf{x})$. Nadalje, to se proširuje na eliptičke Gaussove distribucije u bazi $\{\mathbf{h}_i\}_{i\in[n]}$ tako da imamo vektor $\mathbf{r} = (r_1, \ldots, r_n) \in (\mathbb{R}^+)^n$ za koji vrijedi $r_{j+s_1+s_2} = r_{j+s_1}$, za svaki $j \in [s_2]$. Zatim je uzorak iz $D_\mathbf{r}$ dan s $\sum_{i\in[n]} x_i\mathbf{h}_i$, gdje su x_i odabrani nasumično iz jedno-dimenzionalne Gaussove distribucije $D_{\mathbf{r}_i}$ nad $\mathbb{R}$. Napomenimo da skup označen s $[n]$ označava skup $\{1, \ldots, n\}$.

Definicija 29 (familija distribucija $\Psi_{\leq\alpha}$)**.** *Za* $\alpha \in \mathbb{R}$, $\alpha > 0$, *familija* $\Psi_{\leq\alpha}$ *je skup svih eliptičkih Gaussovih distribucija* $D_\mathbf{r}$ *nad* $K_\mathbb{R}$ *gdje je svaki parametar* $r_i \leq \alpha$.

Sada se još navodi glavni teorem koji dokazuje težinu RLWE problema.

Teorem 4 (vidjeti [13, Teorem 3.6])**.** *Neka je K m-to ciklotomsko polje dimenzije $n = \varphi(m)$ i neka je $R = \mathcal{O}_K$ njegovo polje cijelih brojeva. Neka je $\alpha < \sqrt{\frac{\log n}{n}}$ i neka je $q = q(n) \geq 2$, $q = 1 \bmod m$ poly(n)-ograničen prosti broj takav da $\alpha q \geq \omega(\sqrt{\log n})$. Postoji kvantna redukcija u polinomnom vremenu od $\tilde{O}(\frac{\sqrt{n}}{\alpha})$ SVP na idealnim rešetkama u K do $RDLWE_{q,\Upsilon_\alpha}$. Alternativno, za bilo koji $\ell \geq 1$, može se zamijeniti ciljani problem problemom rješavanja $RDLWE_{q,D_\xi}$ s danih jedino ℓ uzoraka, za $\xi = \alpha \cdot \sqrt[4]{\frac{n\ell}{\log n\ell}}$.*

Tvrdnja Teorema 4 može se iskazati i u sljedećem obliku: Ako postoji algoritam koji može riješiti RDLWE problem, onda postoji kvantni algoritam koji u vremenu $O(q \cdot poly(n))$ rješava SVP problem s faktorom $\tilde{O}(\frac{\sqrt{n}}{\alpha})$.

Izraz $\sqrt[4]{\frac{n\ell}{\log n\ell}}$ u standardnoj devijaciji greške posljedica je pretvaranja eliptičkih distribucija u sfernu. Nije poznato je li ovaj izraz nužan za težinu ili su eliptičke distribucije samo posljedica dokaza.

U prethodnom teoremu, redukcija RDLWE-a se radi s fiksnom distribucijom greške D_ξ umjesto distribucije nad distribucijama grešaka.

Za sada postoji jedino kvantna redukcija $SVP \leq RDLWE$, ali ne i klasična redukcija koja bi bila značajna.

4 Razmjena ključeva prstenastim učenjem s greškama

Opisana razmjena ključeva će se bazirati na ideji autora Jintai Ding, Xiang Xie, Xiaodong Lin u radu [[5], Poglavlje 4, stranice 11-13]. Kako je prstenasto učenje s greškama dosta novi pojam, još uvijek nema nekog standardnog uhodanog načina razmjene ključeva prstenastim učenjem s greškama te razni autori predlažu različite načine. Dodatno, u istome radu autori koriste dosta drugačiju notaciju od prethodnih autora; u ovome radu notacija će biti bazirana na radu [13].

4.1 Protokol za razmjenu ključeva

Protokol za razmjenu ključeva omogućuje različitim korisnicima da sigurno razmjene tajni ključ preko nesigurnog kanala bez da su ranije morali dijeliti tajne materijale i bez da itko tko gleda njihovu komunikaciju može efikasno doznati njihov ključ. Razlika između kriptosustava s javnim ključem i razmjene ključeva je u tome što u kriptosustavima s javnim ključem jedna i druga strana imaju vlastite tajne ključeve koje međusobno ne znaju, a u razmjeni ključeva žele podijeliti tajni ključ.

Glavni razlog zašto još uvijek želimo koristiti protokole za razmjenu ključeva iako postoje kriptosustavi s javnim ključem je taj što su kriptosustavi s javnim ključem sporiji za šifriranje/dešifriranje i pružaju slabiju zaštitu od kriptosustava sa simetričnim ključem. Podsjetimo se iz prethodnih poglavlja, kod LWE smo imali veličinu javnog ključa reda veličine $\mathbb{Z}_q^{n\times n}$ i još smo mogli poslati samo jedan bit, za što je bilo potrebno i n^2 operacija, a da bismo mogli slati više bitova radio bi se čitav postupak ispočetka. Ipak, kod RLWE smo slali n bitova za red veličinu ključeva $\mathbb{Z}_q^n$ i redom veličina $n\log n$ operacija mod-q, što je već dosta efikasnije. Doduše, RLWE je još uvijek manje efikasan od kriptosustava sa simetričnim ključem, pogotovo za slanje velike količine podataka. Tako još uvijek želimo razmijeniti ključeve da bi ih mogli sigurno koristiti kriptosustavi sa simetričnim ključem.

Prvi i najpoznatiji protokol za razmjenu ključeva je **Diffie-Hellman** protokol koji je također dao prvi uzorak za kriptosustave s javnim ključem. Ovdje želimo opisati jedan protokol za razmjenu ključeva sličan Diffie-Hellmanu, ali baziran na RLWE te je dokazivo siguran.

4.2 Ekstraktori, hint i signal funkcije

Na početku uvedimo neke potrebne pojmove kao što su signal funkcije σ_0 i σ_1, hint funkciju S i ekstraktore E za konstrukciju protokola za razmjenu ključeva prstenastim učenjem s greškama.

Definicija 30 (Signal funkcije σ_0 i σ_1)**.** *Za prosti broj $q > 2$, σ_0 i σ_1 se definiraju kao $\sigma_0, \sigma_1 : \mathbb{Z}_q \to \{0,1\}$,*

$$\sigma_0(x) = \begin{cases} 0, & x \in \left[-\lfloor \frac{q}{4} \rfloor, \lfloor \frac{q}{4} \rfloor\right], \\ 1, & \textit{inače}, \end{cases}$$
$$\sigma_1(x) = \begin{cases} 0, & x \in \left[-\lfloor \frac{q}{4} \rfloor + 1, \lfloor \frac{q}{4} + 1 \rfloor\right], \\ 1, & \textit{inače}. \end{cases}$$

Oznaka $b \xleftarrow{\$} \{0,1\}$ označava da je b uniformno nasumično uzorkovan iz skupa $\{0,1\}$.

Definicija 31 (Hint funkcija)**.** *Za proizvoljan $y \in \mathbb{Z}_q$, hint funkcija je $S : \mathbb{Z}_q \to \{0,1\}$, $S(y) = \sigma_b(y)$, za $b \xleftarrow{\$} \{0,1\}$.*

Definicija 32 (Ekstraktori)**.** *Algoritam E je ekstraktor na $\mathbb{Z}_q$ s tolerancijom na grešku δ s obzirom na hint funkciju S ako vrijede sljedeće tvrdnje:*

- *Algoritam E je deterministički i prima ulaz $x \in \mathbb{Z}_q$ i signal $\sigma \in \{0,1\}$ i izlaz mu je $k = E(x, \sigma) \in \{0,1\}$.*
- *Hint algoritam S prima ulaz $y \in \mathbb{Z}_q$ i izlaz mu je $\sigma \leftarrow S(x) \in \{0,1\}$.*
- *Za proizvoljne $x, y \in \mathbb{Z}_q$ takve da je $x - y$ parno i $|x - y| \leq \delta$ vrijedi $E(x, \sigma) = E(\sigma, x)$ za $\sigma \leftarrow S(y)$.*

Ekstraktor se koristi za garanciju točnosti protokola. U protokolu obje strane će računati dvije slične vrijednosti u $\mathbb{Z}_q$. Da bi se složile u zajedničkoj vrijednosti, jedna strana dodatno treba poslati signal svoje vrijednosti pa obje strane računaju zajednički ključ koristeći ekstraktor.

Nadalje, kako imamo definirane signal funkcije, na sljedeći način definiramo ekstraktor preslikavanje $E(a, \sigma) : R_q \leftarrow R_2$, $E(a, \sigma) = (a + \sigma \cdot \frac{q-1}{2} \bmod q) \bmod 2$. Ekstraktor preslikavanje će se koristiti za primanje šumovitih parova vektora i izvlačenja zajedničkog tajnog ključa.

4.3 Protokol za razmjenu ključeva baziran na RLWE

U konstrukciji protokola za razmjenu ključeva, među javnim parametrima generirati ćemo β, koji se ne spominje ranije i n, koji se ne spominje direktno. Tamo su β i ψ u odnosu takvom da je ψ β-ograničen, što znači $Pr\left[||x||_\infty > \beta : x \leftarrow \psi\right] \leq negl(n)$. Drugim riječima, vjerojatnost da je neki element vektora x veći od β, čiji elementi dolaze iz distribucije greške ψ je zanemariva. Iako je β-ograničenost novi pojam u ovome radu, on ne uvodi ništa novo, nego će samo na drugačiji način definirati RLWE problem. Ovdje ga uvodimo samo za potrebe dokaza točnosti razmjene ključa.

Konstrukcija
Opišimo sada kako funkcionira razmjena ključeva.

- Najprije se generiraju javni parametri: q, n, ψ, β, R te još uzorkujemo a iz uniformne distribucije $m \leftarrow R_q$.

- Alice odabire tajni element $s_A \leftarrow \psi$ i $e_A \leftarrow \psi$ pa računa $p_A = as_A + 2e_A \bmod q$ i šalje Bobu.

- Nakon što Bob prima p_A, odabire tajni element i grešku $s_B, e_B^{'} \leftarrow \psi$ te računa $K_B = p_A s_B + 2e_B^{'} \bmod q$ i $\sigma \leftarrow S(K_B)$. Nakon toga odabire $e_B \leftarrow \psi$ i računa $p_B = as_B + 2e_B \bmod q$. Bob šalje (p_B, σ) i dobiva zajednički ključ $SK_B = E(K_B, \sigma)$.

- Nakon što Alice dobije (p_B, σ), uzorkuje svoj $e_A^{'} \leftarrow \psi$ i računa $K_A = s_A p_B + 2e_B^{'} \bmod q$ i dobiva $SK_A = E(K_A, \sigma)$.

Prije leme o vjerojatnosti za dobru razmjenu ključeva i modificiranog teorema za problem RLWE koji u sebi koristi β-ograničenost je potreban pojam ogromne (eng. overwhelming) i zanemarive vjerojatnosti. Događaj E ima zanemarivu vjerojatnost ako postoji zanemariva funkcija $\mu : \mathbb{N} \to \mathbb{R}$ takva da se događaj E pojavljuje vjerojatnošću manjom od one koju daje zanemariva funkcija μ, tj. $Pr(A(n)) \leq \mu(n)$. Događaj ima ogromnu vjerojatnost da se dogodi, analogno kao i u definiciji ogromnih funkcija u Poglavlju 3.1, ako se uvijek događa osim sa zanemarivom vjerojatnošću.

Modificirajmo definiciju RLWE problema i glavni Teorem 4 da bude u skladu s $\beta-$om korištenom u ovom poglavlju:

Definicija 33 (RLWE, varijanta odluke za protokol)**.** *Neka je* Υ *β-ograničena distribucija nad familijom distribucija greški, svaka nad* $K_{\mathbb{R}}$*. Varijanta odluke RLWE problema, označena* $RDLWE_{q,\Upsilon}$ *(eng. ring-decision learning with errors) je raspoznati između proizvoljno mnogo nezavisnih uzoraka iz* $A_{s,\psi}$ *za nasumičan odabir* $(s,\psi) \leftarrow U(R_q^\vee) \times \Upsilon$ *i istog broja uniformno nasumičnih i nezavisnih uzoraka iz* $R_q \times \mathbb{T}$*.*

Navodimo teorem koji dokazuje težinu RLWE problema koristeći β-ograničenost.

Teorem 5 (vidjeti[5, Teorem 2])**.** *Neka je* $R = \mathbb{Z}[x]/f(x)$ *prsten,* $f(x) = x^n + 1$*, za* n *potenciju broja 2,* q *prosti broj takav da je* $q = q(n) = 1 \ mod\ 2n$ *i* $\beta = \omega(\sqrt{\log n})$*. Postoji efikasno uzorkovana distribucija* ψ *koja daje element prstena* R *s normom manjom od* β *s ogromnom vjerojatnošću takva da ako postoji efikasan algoritam koji rješava* $RLWE^{(m)}_{n,q,\psi}$*, onda postoji efikasan kvantni algoritam za rješavanje* $n^{2.5} \cdot (\frac{q}{\beta}) \cdot \sqrt{(\frac{nm}{\log nm})}$ *aproksimacijskog najgoreg slučaja* SVP *za idealne rešetke nad* R*.*

Ranije smo naveli da razmjena ključeva ne radi točno u svim slučajevima, nego je samo jako vjerojatna da radi dobro. Sada navedimo lemu koja definira poželjne parametre da bi razmjena ključeva bila točna u što više slučajeva.

Lema 4 (vidjeti [5, Lema 9])**.** *Ako je* $8n\beta^2 \leq \frac{q}{2} - 2$*, onda* $SK_A = SK_B$ *s ogromnom vjerojatnošću.*

Parametri i kriva razmjena

Sada navedimo s kojim parametrima u kojim varijantama RLWE protokola dolazi do pogrešne razmjene ključa. Eksperimentalno, s mojim podacima i podacima iz rada [20], utvrđeno je da u navedenom protokolu dolazi do manje greške s većim brojevima. U navedenom radu se za parametre $n = 512$ i $q = 25601$ dobiva kriva razmjena s vjerojatnošću 2^{-71}, a za $n = 1024$ i $q = 40961$ dobiva se kriva razmjena s vjerojatnošću 2^{-91}.

U mojim podacima kojima će se testirati točnost razmjene ključeva; svi testovi će se raditi na 500 000 testova razmjene. Za $n = 128$ i $q = 2^{32} - 1$ dobiva se krivi rezultat s vjerojatnošću 2^{-11}; do krive razmjene je došlo 247 puta. S $n = 64$ i $q = 2^{16} - 1$ dobiva se krivi rezultat s vjerojatnošću $2^{-7.35}$; do krive razmjene je došlo 3064 puta. Za $n = 64$ i za $q = 2^8 - 1$ dobiva se krivi rezultat s vjerojatnošću 0.82; do krive razmjene je došlo 413422 puta. Za $n = 256$ i za $q = 2^{16} - 1$ dobiva se krivi rezultat s vjerojatnošću manjom od $\frac{1}{500000} \approx 2^{-19}$; niti jednom nije došlo do krive razmjene.

Literatura

[1] G. Brookfield, *The Coefficients of Cyclotomic Polynomials*, 2016.
Dostupno na "https://www.calstatela.edu/sites/default/files/cyclotomic.pdf".

[2] W. Beullens, *Breaking Rainbow Takes a Weekend on a Laptop*, 2022.
Dostupno na "https://eprint.iacr.org/2022/214.pdf". - probijanje duge

[3] W. Castryck, T. Decru, *An efficient key recovery attack on SIDH*, 2022.
Dostupno na "https://eprint.iacr.org/2022/975.pdf". - probijanje SIDH-a.

[4] K. Conard, *The Different Ideal*
Dostupno na "https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf".

[5] J. Ding, X. Xie, X. Lin, *A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem*, 2012.
Dostupno na "https://eprint.iacr.org/2012/688.pdf".

[6] L. Ducas, A. Durmus, *Ring-LWE in Polynomial Rings.*
Dostupno na "https://homepages.cwi.nl/~ducas/RLWE/RLWE.pdf"

[7] S. Dufresne, *The Enigma Enigma, How the Enigma Machine Worked*, 2017.
Dostupno na "https://hackaday.com/2017/08/22/the-enigma-enigma-how-the-enigma-machine-worked/". - slika ključeva enigme.

[8] A. Dujella, *Teorija brojeva* , Školska knjiga, Zagreb, 2019.

[9] N. Dwarakanath, S. Galbraith, *Sampling from Discrete Gaussians for Lattice-Based Cryptography on a Constrained Device*, 2014.
Dostupno na "https://www.math.auckland.ac.nz/~sgal018/gen-gaussians.pdf".

[10] M. R. Garel, D. S. Johnson,*Compuers and Intractability: A Guide to the Theory of NP-Completeness*, 1979.

[11] D. Goodin, *Post-quantum encryption contender is taken out by single-core PC and 1 hour*, 2022.
Dostupno na "https://arstechnica.com/information-technology/2022/08/sike-once-a-post-quantum-encryption-contender-is-koed-in-nist"\
"-smackdown/".

[12] A. Kipnis, J. Patarin, L. Goubin, *Unbalanced Oil and Vinegar Signature Schemes*.

[13] V. Lyubashevsky, C. Peikert, O. Regev, *On Ideal Lattices and Learning with Errors Over Rings*, 2013. (prva verzija je iz 2010.).
Dostupno na "https://eprint.iacr.org/2012/230.pdf".

[14] D. Micciancio, *Lattice-based Cryptography*, 2008.
Dostupno na "https://cims.nyu.edu/~regev/papers/pqc.pdf".

[15] B. Pavković, D. Veljan, *Elementarna matematika 1* , Školska knjiga, 2004.

[16] C. Peikert, *Lattices in Cryptography, Lecture 1, Mathematical Background, 2013.* Dostupno na "https://web.eecs.umich.edu/~cpeikert/lic13/lec01.pdf".

[17] C. Peikert, *Lattice Cryptography for the Internet*.
Dostupno na "https://www.youtube.com/watch?v=uycY1O9f2Nw".

[18] O. Regev, *On Lattices, Learning with Errors, Random Linear Codes, and Cryptography*.
Dostupno na "https://web.archive.org/web/20170810050443/http://www.cs.au.dk/~stm/local-cache/regev-on-lattices.pdf".

[19] O. Regev, *Lattices in Computer Science, Lecture 8: Dual Lattices*, 2004.
Dostupno na "https://cims.nyu.edu/~regev/teaching/lattices_fall_2004/ln/DualLattice.pdf".

[20] V. Singh, *A Practical Key Exchange for the Internet using Lattice Cryptography*, 2015.
Dostupno na "https://eprint.iacr.org/2015/138.pdf". - Kriva razmjena ključa.

Sažetak

Tema ovog rada je opisati kako se tajni ključevi mogu razmijeniti preko nesigurnog kanala pomoću tehnike prstenastog učenja s greškama. Prije toga opisani su potrebni algebarski pojmovi za definiciju. Također, opisano je i prstenasto učenje s greškama kao kriptosustav s asimetričnim ključem, a i nešto o povijesti i o njegovom prethodniku, učenju s greškama.

Ključne riječi

kriptografija, post-kvantna kriptografija, asimetrični kriptosustav, prstenasto učenje s greškom, kriptografija bazirana na rešetkama

Ring learning with errors - key exchange

Summary

The topic of this paper is to describe how secret keys can be exchanged over a non-secure channel using Ring Learning with Errors. Before that, we describe the necessary terms for the definition from algebra, and we also describe Ring Learning with Errors as a public-key cryptosystem and some history about the predecessor Learning with Errors.

Keywords

cryptography, post-quantum cryptography, public-key cryptosystem, ring learning with error, lattice-based cryptography

Životopis

Rođen sam u Bjelovaru 1998. godine te sam u istom gradu išao u osnovnu i srednju školu. Godine 2018. upisujem se na prediplomski studij matematike i računarstva na Odjelu za matematiku u Osijeku. 2021. godine upisao sam diplomski studij matematike, smjer: matematika i računarstvo.