Kriptografija temeljena na grafovima izogenija supersingularnih eliptičkih krivulja

Marević, Maja

Kriptografija temeljena na grafovima izogenija supersingularnih eliptičkih krivulja

Marević, Maja

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Maja Marević

KRIPTOGRAFIJA TEMELJENA NA GRAFOVIMA IZOGENIJA SUPERSINGULARNIH ELIPTIČKIH KRIVULJA

Diplomski rad

Voditelj rada:
Izv.prof.dr.sc Matija Kazalicki

Zagreb, rujan, 2020.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Mojoj majci. Hvala ti na svakoj poruci ohrabrenja, neizmjernoj brizi i najtoplijem zagrljaju ovog svijeta. Tati. Hvala ti na vjerovanju da ja to mogu i da će 'tvoja ćer' to riješiti. Mati. Hvala ti na utješnom humoru i tihoj brizi. Hvala vam! Na bezuvjetnoj ljubavi, svim odricanjima i riječima utjehe.

Marinu. Jer je Marin. Jer je zbog njega sve lakše i ljepše. Hvala ti. Za sve izgovoreno i neizgovoreno. Zorici. Na slatkim porukama prije svakog ispita i vjerovanju u mene. Hvala ti što nikad ne zaboravljaš. Antei, Luki i Matei. Hvala vam što ste uvijek tu.

Ani. Jer je dala sve od sebe da skupa uspijemo. Hvala ti za kasna tipkanja, sve materijale, obavijesti i zajednička učenja! Karlu i Heleni. Na svemu. Jer je bilo savršeno i bez kuhala za vodu. Ani i Juri, jer su me dizali nakon mojih prvih 'padova'. Dragi, Ninu i Tomi. Na bezuvjetnoj podršci, pomoći i toploj riječi. I svima vama koji ste rasli sa mnom. Hvala!

Mentoru. Na vremenu, strpljenju i pomoći. Na prijenosu znanja i sveukupnom trudu. Hvala Vam!

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

Uvod

Zaštitu podataka, skrivanja i maskiranja informacija zbog raznih taktika i vlastite sigurnosti možemo pronaći još u dalekoj povijesti. S vremenom i razvojem tehnologije javljala se sve veća potreba za sigurnom, neometanom i zaštićenom komunikacijom. Znanstvena disciplina koja se bavi logičkom promjenom podataka kako bi osigurala da izvorni podatci ostanu poznati isključivo primatelju i pošiljatelju naziva se **kriptografija**.

U klasičnoj kriptografiji sigurnost ovisi o tajnom ključu. No, u situacijama kad ne postoji mogućnost razmjene ključeva sigurnim komunikacijskim kanalom oslanjamo se na kriptosustave s javnim ključem. Prvi, najpopularniji i najkorišteniji kriptosustav s javnim ključem je **RSA kriptosustav** kojeg su 1977.godine izumili Ron Rivest, Adi Shamir i Leonard Adleman. Sigurnost RSA kriptosustava zasnovana na teškoći faktorizacije velikih prirodnih brojeva. Važno je pitanje što bi se dogodilo sa sigurnošću RSA kriptosustava (i ostalih kriptosustava s javnim ključem) ako bi se uspjela konstruirati efikasna kvantna računala.

Već desetljećima znanstvenici diljem svijeta pokušavaju izgraditi kvantna računala. Ideja iza kvantnog računala je koristiti teoriju kvantne mehanike i na tome temeljiti funkcioniranje računala. U klasičnim računalima, podatci su enkodirani u bit-ove (binarni bit-ovi, od kojih je svaki 0 ili 1). U kvantnim računalima koriste se qbit-ovi (quantum bits) koji nemaju determinističko stanje, nego uzimaju spektar vrijednosti u isto vrijeme. Koristeći rječnik kvantne teorije, oni su u kvantnoj superpoziciji[1]. Razumijevanjem pojmova qubita i superpozicije iz domene kvantne mehanike razvila se ideja o izradi kvantnog računala koje bi obavljalo određene zadatke neusporedivo brže od klasičnih računala. Upravo jedan takav zadatak bio bi i traženje prostih faktora zadanog broja poznat pod nazivom **Shorov algoritam**. Shorov algoritam koristi činjenicu da kvantne metode omogućavaju vrlo brzo računanje perioda periodičnih funkcija. To daje polinomijalne kvantne algoritme za probleme faktorizacije i diskretnog logaritma. U takvoj okolini, kriptosustavi javnog ključa zasnovani na faktorizaciji (RSA, Rabin) i problemu diskretnog logaritma (ElGamal, ECC) postali nesigurni i neupotrebljivi.

[1]Kvantna superpozicija je osnovni princip kvantne mehanike, po kojem se, poput valova u "klasičnoj" fizici, bilo koja dva (ili više) kvantnih stanja mogu dodati ("superponirati"), te će rezultat biti valjano kvantno stanje; i obrnuto, svako kvantno stanje se može predstaviti kao zbroj dva ili više posebna stanja

Posljedično, stvoreno je polje post-kvantne kriptografije (PQC[2]) koje za cilj ima razviti i implementirati algoritme koji se odupiru kriptoanalizi od strane klasičnih i kvantnih računala.

U ovom radu, proučavat ćemo algoritam za koji se vjeruje da je kvantno otporan i da može biti korišten u post-kvantnoj eri (ako ista postane realnost). Algoritam SIDH (Supersingular Isogeny Diffie Hellman) je razmjena ključeva čija je metoda bazirana na Diffie-Hellmanovoj razmjeni. U SIDH-u, početni javni parametri su **supersingularne** eliptičke krivulje, koje ćemo u sljedećim poglavljima i definirati. Za razliku od Diffie-Hellmanovih eliptičkih krivulja, u SIDH-u se ne biraju elementi iz grupe eliptičke krivulje već se računaju izogene krivulje iste. Dakle, biraju se elementi iz takozvanog grafa izogenija, čiji su vrhovi eliptičke krivulje, a bridovi izogenije.

U sljedeća dva poglavlja definirani su svi pojmovi potrebni za razumijevanje SIDH algoritma, dok četvrto poglavlje opisuje SIDH algoritam i njegovu sigurnost temeljenu na pet složenih problemima. Iako desetljeće mlađi i manje testiran od svih navedenih, trenutna slika sigurnih svojstava SIDH algoritma izgleda obećavajuće.

[2]Post-quantum cryptography

Poglavlje 1

Eliptičke krivulje u kriptografiji

1.1 Definicija i osnovna svojstva eliptičkih krivulja

Definicija 1.1.1 (Eliptička krivulja)**.** *Neka je $\mathbb{K}$ polje. Eliptička krivulja nad poljem $\mathbb{K}$ je nesingularna projektivna kubna krivulja nad $\mathbb{K}$ s barem jednom ($\mathbb{K}$-racionalnom) točkom. Ona ima (afinu) jednadžbu oblika*

$$F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0, \tag{1.1}$$

gdje su koeficijenti $a, b, c, ..., j \in \mathbb{K}$.

Nesingularnost znači da je u svakoj točki na krivulji, promatranoj u projektivnoj ravnini $\mathbb{P}^2(\overline{\mathbb{K}})$ nad algebarskim zatvorenjem od $\mathbb{K}$, barem jedna parcijalna derivacija funkcije F : $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ različita od 0. Geometrijski, nesingularnost znači da nema "šiljaka" te da ne postoje izolirane točke ili točke u kojima se krivulja siječe sama sa sobom. Svaka jednadžba oblika (1.1) može se transformacijama svesti na oblik

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2}$$

koji nazivamo **generalizirana Weierstrassova forma**. Oblik (1.2) koristi se u poljima karakteristike[1] 2 ili 3. Eliptičke krivulje u takvim poljima popularne su u kriptografiji jer se njihova aritmetika može učinkovitije implementirati na računala.

Neka je $\mathbb{K}$ polje karakteristike različite od 2. Nadopunjavanjem na potpuni kvadrat jednadžba (1.2) može se svesti na oblik

$$E : y^2 = 4x^3 + b_2x^2 + b_4x + b_6 \tag{1.3}$$

[1]Karakteristika polja $\mathbb{K}$ je najmanji prirodni broj n takav da je $1 + 1 + ... + 1 = n \cdot 1 = 0$, gdje su 0 i 1 neutralni elementi za zbrajanje, odnosno množenje u $\mathbb{K}$.

gdje je

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6. \tag{1.4}$$

Definiramo još i $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. Ukoliko je karakteristika od $\mathbb{K}$ različita i od 3, daljnim transformacijama dobivamo jednadžbu oblika

$$y^2 = x^3 - 27c_4 - 54c_6 \tag{1.5}$$

gdje je

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \tag{1.6}$$

Sada definiramo dvije osnovne konstante koje vežemo uz takve eliptičke krivulje i Weierstrassovu jednadžbu.

Definicija 1.1.2. ***Diskriminanta*** $\triangle$ *Weierstrassove jednadžbe dana je sa*

$$\triangle = \triangle(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \tag{1.7}$$

dok je ***j-invarijanta*** *eliptičke krivulje jednaka*

$$j = j(E) = \frac{(b_2^2 - 24b_4)^3}{\triangle} \tag{1.8}$$

Općenito se diskriminanta polinoma f stupnja n s vodećim koeficijentom a_n i korijenima $x_1, ..., x_n$ (iz $\overline{\mathbb{K}}$) definira kao

$$\mathrm{Dis}(f) = a_n^{2n-2} \prod_{i<j}^{n} (x_i - x_j)^2 \tag{1.9}$$

i jednaka je 0 ako i samo ako f ima višestrukih nultočaka. Kao što smo spomenuli ranije, krivulja je nesingularna ako i samo ako $\triangle \neq 0$. Prepostavimo li dodatno da je karakteristika polja $\mathbb{K}$ različita i od 2 i od 3, Weierstrassovu jednadžbu možemo pojednostaviti :

$$E : y^2 = x^3 + ax + b \tag{1.10}$$

gdje su $a, b \in \mathbb{K}$ zajedno s elementom označenim O koji nazivamo "točka u beskonačnosti". Takav oblik jednadžbe eliptičke krivulje nazivamo **kratka Weierstrassova jednadžba**. Uvjet nesingularnosti je sada da kubni polinom $f(x) = x^3 + ax + b$ nema višestrukih nultočaka, što je ekvivalentno uvjetu da je diskriminanta $D = -4a^3 - 27b^2$ različita od 0. Uz Weierstrassovu jednadžbu oblika (1.10) diskriminanta je oblika

$$\triangle = -16(4a^3 + 27b^2) \tag{1.11}$$

dok je j-invarijanta jednaka

$$j = -1728\frac{(4a)^3}{\triangle} \tag{1.12}$$

j-invarijanta je usko povezana s pojmom izomorfizma eliptičkih krivulja.

Definicija 1.1.3. *Dvije eliptičke krivulje definirane Weierstrassovim jednadžbama E (s varijablama x, y) i E' (s varijablama x', y') su izomorfne nad $\mathbb{K}$ ako i samo ako postoje konstante $r, s, t \in \mathbb{K}$ i $u \in \mathbb{K}^*$ takve da dopustivom zamjenom varijabli*

$$x = u^2x' + r, \qquad y = u^3y' + su^2x' + t \tag{1.13}$$

jednadžbu E transformiramo u E'.

Ova transformacija je reverzibilna i njen inverz također definira dopustivu zamjenu varijabli koja E' pretvara u E. Slijedi iskaz leme koja govori da j-invarijanta karakterizira klasu ekvivalencije ove relacije nad algebarskim zatvorenim poljem $\overline{\mathbb{K}}$.

Lema 1.1.4. *Dvije izomorfne eliptičke krivulje nad poljem $\mathbb{K}$ imaju jednaku j-invarijantu. Vrijedi obrat, dvije krivulje s jednakom j-invarijantom su izomorfne nad $\overline{\mathbb{K}}$.*

Objasnimo još pojam "točke u beskonačnosti". Prikažemo li eliptičku krivulju u projektivnoj ravnini, točka u beskonačnosti pojavljuje se prirodno. Projektivnu ravninu $\mathbb{P}^2(\overline{\mathbb{K}})$ dobijemo tako da na skupu $\mathbb{K}^3\backslash\{(0,0,0)\}$ uvedemo relaciju ekvivalenciju $(X, Y, Z) \sim (kX, kY, kZ), k \in \mathbb{K}, k \neq 0$. Ako u (afinoj) jednadžbi eliptičke krivulje uvedemo supstituciju $x = \frac{X}{Z}, y = \frac{Y}{Z}$ dobivamo projektivnu jednadžbu

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{1.14}$$

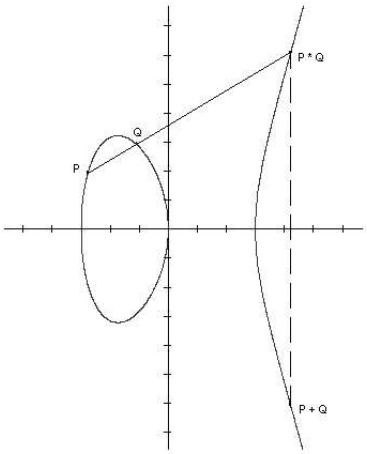
Ukoliko je $Z \neq 0$, klasa ekvivalencije (X, Y, Z) ima reprezentant $(x, y, 1)$ pa tu kasu možemo identificirati s (x, y). Međutim, postoji i klasa ekvivalencije koja sadrži točke za koje je $Z = 0$. Ona ima reprezentant $(0, 1, 0)$ i tu klasu identificiramo s točkom u beskonačnosti O.

Zbrajanje točaka na eliptičkim krivuljama

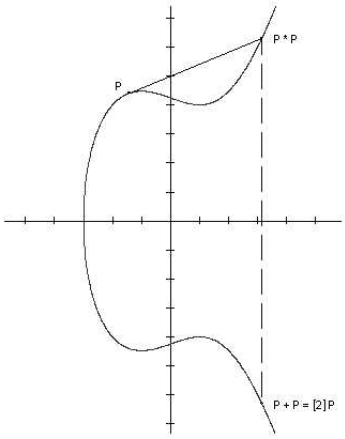
Neka je E eliptička krivulja koju smo prethodno definirali. Skup točaka krivulje E možemo prikazati kao grupu s operacijom $\oplus$ koju zovemo zbrajanje.

Geometrijski opis Neka su P i Q dvije različite točke na eliptičkoj krivulji E. Povučemo li pravac koji spaja te dvije točke, s obzirom na to da se radi o kubnoj krivulji, dobit ćemo novu točku u kojoj pravac presijeca krivulju E. Nazovimo je R. Zrcalimo li točku R preko x osi, dobivamo novu točku na krivulji E koju možemo označiti s $P + Q$.
Nadalje, promatramo slučaj zbrajanja dvije iste točke. Da bi točku P dodali samoj sebi, provučemo tangentu na krivulju E u točki P. Tangenta presijeca $E(K)$ u još jednoj točki, R. Zrcalimo li ponovno točku R preko x-osi, dobivamo točku $[2]P = P + P$. Ako je povučena tangenta u točki vertikalna, ona presijeca krivulju u točki beskonačnosti i tada je $P+P = O$.

Izvedimo sada formalni iskaz definicije zbrajanja točaka eliptičke krivulje. Neka su $P = (x_1, y_1)$ i $Q = (x_2, y_2)$ točke krivulje E takve da $x_1 \neq x_2$. Cilj je dobiti zbroj točaka P i



(a) Zbrajanje točaka P, Q na eliptičkoj krivulji



(b) Dupliciranje točke P na eliptičkoj krivulji

Slika 1.1: Računske operacije na eliptičkoj krivulji

Q, $R = P \oplus Q = (x_3, y_3)$. Pravac koji prolazi kroz P i Q ima koeficijent smjera:

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2} \tag{1.15}$$

Uvrštavanjem jednadžbe pravca kroz točku P, tj $y = \lambda(x - x_1) + y_1$ u jednadžbu eliptičke krivulje te izjednačavanjem koeficijenata uz x^2 u $x^3 + ax + b - (\lambda(x - x_1) + y_1)^2 = (x - x_1)(x - x_2)(x - x_3)$ dobivamo

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = -y_1 + \lambda(x_1 - x_3) \tag{1.16}$$

Definicija 1.1.5. *Neka je $P = (x_1, y_1), Q = (x_2, y_2)$. Tada je*

1) $-O = O$

2) $-P = (x_1, -y_1)$

3) $O + P = P$

4) ako je $Q = -P$, onda je $P + Q = O$

5) ako je $Q \neq -P$, onda je $P + Q = (x_3, y_3)$, gdje je

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = -y_1 + \lambda(x_1 - x_3) \tag{1.17}$$

gdje je

$$\begin{aligned} \lambda &= \frac{y_2 - y_1}{x_2 - x_1}, \quad x_1 \neq x_2 \\ \lambda &= \frac{(3x_1^2 + a)}{2y_1}, \; x_1 = x_2 \end{aligned} \tag{1.18}$$

Ovako definirano zbrajanje na E je Abelova[2] grupa, s obzirom na to fNda vrijedi komutativnost, "točka u beskonačnosti" je neutralni element i postoji inverz. Također, vrijedi i asocijativnost, ali je složenija za dokazati. Valja napomenuti da su analitički izrazi za zbrajanje na eliptičkoj krivulji nad poljima karakteristike 2 ili 3 slični, uz male modifikacije.

Višekratnike točke P označujemo s $m[P]$ te ih računamo koristeći već znane formule za zbrajanje točaka :

$$(x_3, y_3) = ((\lambda^2 - x_1 - x_2)\text{mod n}, (\lambda(x_1 - x_3) - y_1)\text{mod n}), \tag{1.19}$$

pri čemu je $\lambda = \frac{(3x_1^2+a)}{2y_1}$ (mod n) ako su točke jednake, odnosno $\lambda = \frac{y_1-y_2}{x_1-x_2}$ (mod n) ukoliko su točke različite.

1.2 Eliptičke krivulje nad konačnim poljem

Konačna polja

Konačno polje s q elemenata označavat ćemo s $\mathbb{F}_q$. Konačno polje ne može biti karakteristike 0, stoga neka je p karakteristika od $\mathbb{F}_q$. Tada $\mathbb{F}_q$ sadrži prosto polje[3] $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Nadalje, $\mathbb{F}_q$ je konačno dimenzionalan vektorski prostor nad $\mathbb{F}_p$. Neka je k njegova dimenzija, $\{e_1, ..., e_k\}$ njegova baza. Tada se svaki element $a \in \mathbb{F}_q$ može na jedinstven način prikazati u obliku linearne kombinacije

$$a = \lambda_1 e_1 + ... + \lambda_k e_k \tag{1.20}$$

gdje su $\lambda_i \in \mathbb{F}_p$. Tako, svakom $a \in \mathbb{F}_q$ možemo bijektivno pridružiti uređenu k-torku $(\lambda_1, ..., \lambda_k) \in (\mathbb{F}_p)^k$. Stoga je $q = p^k$.

Vrijedi i obrat : za svaku potenciju prostog broja $q = p^k$ postoji polje od q elemenata i ono je jedinstveno do na izomorfizam.

Elementi polja $\mathbb{F}_q$ različiti od nule tvore Abelovu grupu s obzirom na množenje. Tu grupu označavamo s $\mathbb{F}_q^*$. Iz Lagrangeovog[4] teorema slijedi da red svakog elementa $a \in \mathbb{F}_q^*$ dijeli $q - 1$. Grupa $\mathbb{F}_q^*$ je ciklička.

Za daljnu analizu, potrebne su nam definicije ideala i kvocijentnog prstena.

---

[2]Grupa G je Abelova ili komutativna grupa ako za svaki $x, y \in G$ vrijedi $x \cdot y = y \cdot x$.

[3]Polje koje ne sadrži niti jedno drugo polje. Pokazuje se da su,do na izomorfizam, jedina prosta polja $\mathbb{Q}$ i $\mathbb{Z}/p\mathbb{Z}$.

[4]Za svaku konačnu grupu G i za svaku podgrupu H od G vrijedi : $|G| = [G : H] \cdot |H|$, gdje je$[G : H]$ indeks podgrupe H u G, točnije broj lijevih klasa. Odnosno, za svaku konačnu grupu G red (broj elemenata) podgrupe H od G dijeli red od G.

Definicija 1.2.1. *Neprazan podskup I prstena R naziva se **ideal** ako vrijedi*

(i) $a - b \in I$, *za svaki* $a, b \in I$

(ii) $ra \in I$, *za svaki* $a \in I, r \in R$.

Definicija 1.2.2. *Neka je I ideal u prstenu R i neka je* $R/I = \{a + I | a \in R\}$. *Tada se prsten* $(R/I, +, \cdot)$ *naziva **kvocijentni prsten** R modulo I.*

Polje $\mathbb{F}_q$ za $q = p^k$ možemo realizirati kao kvocijentni prsten $\mathbb{F}_p[t]/(g(t))$, gdje je $g(t)$ neki normirani ireducibilan[5] polinom stupnja k u $\mathbb{F}_p[t]$. Elemente ovog polja može se prikazati kao polinome nad $\mathbb{F}_p$ stupnja $\leq k-1$, dok se pripadne operacije zbrajanja i množenja polinoma nasljeđuju iz $\mathbb{F}_p[t]$, s tim da se nakon množenja računa ostatak pri dijeljenju s polinomom $g(t)$. Da bi operacije u polju $\mathbb{F}_q$, neophodne za računanje s točkama na eliptičkoj krivulji nad ovim poljem, bile što efikasnije, obično se polinom $g(t)$ bira tako da ima što manju težinu W(broj koeficijenata različitih od 0). U slučaju $q = 2^k$ koji je najzanimljiviji za primjene u kriptografiji, čini se da je uvijek moguće postići da je $W = 3$ ili $W = 5$. Primjerice, u šifriranju pomoću Advanced Encryption Standarda (AES) koristi se polje $\mathbb{F}_{2^8}$ definirano pomoću ireducibilnog polinoma $x^8 + x^4 + x^3 + x + 1$.
Eliptičke krivulje koje se koriste u kriptografiji definirane su s dva tipa konačnih polja :

- polje $\mathbb{F}_p$ gdje je $p > 3$ prost broj
- polje $\mathbb{F}_{2^m}, m \in \mathbb{N}$

Polje $\mathbb{F}_p$

Polje $\mathbb{F}_p$ sastoji se od p elemenata $\{0, 1, ..., p-1\}$ gdje su operacije zbrajanja i množenja definirane na sljedeći način :

- *Zbrajanje* : Neka su $a, b \in \mathbb{F}_p$. Tada je $a + b = r \in \mathbb{F}_p$, gdje je $r \in [0, p-1]$ ostatak pri dijeljenju cijelog broja $a + b$ i p. Kraće zapisano, $a + b = r \bmod p$.
- *Množenje* : Neka su $a, b \in \mathbb{F}_p$. Tada je $a \cdot b = s \in \mathbb{F}_p$ gdje je $s \in [0, p-1]$ ostatak pri dijeljenju cijelog broja, tj. $a \cdot b = s \bmod p$.

Neutralni element zbrajanja u $\mathbb{F}_p$ je 0, neutralni element množenja je 1.

[5]Neka je F polje. Kažemo da je polinom $f(x) \in F[x]$ ireducibilan nad poljem F ako je $deg(f(x)) \geq 1$ i

$$f(x) = g(x)h(x), \quad g(x), h(x) \in F[x]$$

povlači $g(x) \in F$ ili $h(x) \in F$.

Polje $\mathbb{F}_{2^m}$

Polje $\mathbb{F}_{2^m}$ je polje karakteristike 2 i sastoji se od 2^m elemenata. Zbrajanje i množenje definirani su pomoću ireducibilnog polinoma $P(X)$ stupnja m. Polinom se bira sa što manjom težinom W.
Zbrajanje Neka su $A(x)$ i $B(x)$ polinomi iz $\mathbb{F}_{2^m}$. Suma ta dva elementa računa se kao :

$$S(x) = A(x) + B(x) = \sum_{i=0}^{m-1}(a_i + b_i)x^i (\text{mod } 2) \tag{1.21}$$

Množenje Umnožak polinoma $A(x).B(x)$ je polinom $U(x)$ koji predstavlja ostatak pri dijeljenju standardnog umnoška polinoma $C(x) = A(x) \cdot B(x)$ polinomom $P(x)$. Odnosno

$$U(x) = A(x) \cdot B(x) \bmod P(x) \tag{1.22}$$

Grupa $E(\mathbb{F}_p)$

Ponovimo, eliptička krivulja nad poljem $\mathbb{F}_p$ je skup točaka $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ koje zadovoljavaju jednadžbu $E : y^2 = x^3 + ax + b$ zajedno s "točkom u beskonačnosti" $\mathcal{O}$. Takav skup označavamo s $E(\mathbb{F}_p)$. Vrijede svi prethodno nabrojani analitički izrazi za zbrajanje na eliptičkoj krivulji (1.1.5) modulo p, uz iznimku za $p = 3$. U tom slučaju, jednadžba eliptičke krivulje je oblika $E : y^2 = x^3 + ax^2 + bx + c$.

Primjer 1.2.3. *Promotrimo eliptičku krivulju*

$$E : y^2 = x^3 + x + 1 \tag{1.23}$$

nad poljem $\mathbb{F}_7$. *Odredimo elemente i strukturu grupe* $E(\mathbb{F}_7)$.

Rješenje. Jedini kvadrati u polju $\mathbb{F}_7$ su $0, 1, 2$ i 4. Uvrstimo li $x = 0, 1, 2, 3, 4, 5, 6$ u jednadžbu krivulje E dobivamo redom jednadžbe $y^2 = 1, 3, 4, 3, 6, 5, 6$ u $\mathbb{F}_7$ gdje za samo $x = 0, 2$ i pripadne jednadžbe imaju rješenja.

Dobivamo :

$$E(F_7) = \{\mathbb{O}, (0, 1), (0, 6), (2, 2), (2, 5)\}. \tag{1.24}$$

Nadalje, određujemo strukturu grupe $E(\mathbb{F}_7)$. Uzmimo točku $P = (0, 1)$ i izračunajmo njezine višekratnike. Imamo :

$$[2]P = (2, 5), \quad [3]P = (2, 2), \quad [4]P = (0, 6), \quad [5]P = \mathcal{O} \tag{1.25}$$

Dakle, $E(\mathbb{F}_7)$ je ciklička grupa reda 5, a točka P joj je generator [6].

[6]Grupa G je ciklička grupa ukoliko postoji element $x \in G$ takav da je $G = \{x^k | \ k \in \mathbb{Z}\}$. Takav element nazivamo generator grupe i označavamo s $\langle x \rangle = G$.

x	y^2	y	Točka
0	1	±1	(0,1) (0,6)
1	3	-	-
2	4	±2	(2,2) (2,5)
3	3		-
4	6	-	-
5	5	-	-
6	6	-	-
∞	∞	∞	∞

Grupa $E(\mathbb{F}_{2^m})$

Svaka eliptička krivulja nad poljem $\mathbb{F}_{2^m}$ karakteristike 2 može se transformirati u jedan od sljedećih oblika:

$$y^2 + Cy = x^3 + ax + b \qquad \text{ili} \qquad y^2 + xy = x^3 + ax + b \tag{1.26}$$

Krivulje čije točke zadovoljavaju jednadžbu prvog oblika nazivamo **supersingularne krivulje**, o kojima ćemo kasnije reći nešto više. Eliptička krivulja nad poljem $\mathbb{F}_{2^m}$ je skup točaka $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ koje zadovoljavaju jednadžbu $E : y^2 + xy = x^3 + ax + b$ zajedno s "točkom u beskonačnosti" O. Takav skup označavmo s $E(\mathbb{F}_{2^m})$. Iskažimo formule za zbrajanje točaka na eliptičkoj krivulji nad poljem $\mathbb{F}_{2^m}$.

Neka je $P = (x_1, y_1)$ i $Q = (x_2, y_2)$, tada je $-P = (x_1, x_1 + y_1)$ te $P + Q = (x_3, y_3)$, $P + P = [2]P = (x_p, y_p)$ gdje su :

$$\begin{aligned} x_3 &= \lambda^2 + \lambda + x_1 + x_2 + a \quad \text{i} \quad y_3 = \lambda(x_1 + x_3) + x_3 + y_1, \quad \text{za} \quad \lambda = \frac{y_1 + y_2}{x_1 + x_2} \\ x_p &= \delta^2 + \delta + a = x_1^2 + \frac{b}{x_1^2} \quad \text{i} \quad y_p = x_1^2 + \delta x_3 + x_3, \qquad \text{za} \quad \delta = \frac{x_1 + y_1}{x_1} \end{aligned} \tag{1.27}$$

$E(\mathbb{F}_{2^m}, +)$ je Abelova grupa. Postavlja se pitanje što se može općenito reći o grupi $E(\mathbb{F}_q)$, tj. o njezinom redu $|E(\mathbb{F}_q)|$ i strukturi.

Red grupe $E(\mathbb{F}_q)$

Lako je zaključiti da je $|E(\mathbb{F}_q)| \in [1, 2q + 1]$. Naime, na E imamo točku O, a pored toga svakom od q mogućih x-eva odgovaraju najviše dva y-a. No, samo pola elemenata od $\mathbb{F}_q$ imaju kvadratni korijen (to su elementi oblika g^{2n}, gdje je g generator grupe $\mathbb{F}_q$), pa možemo očekivati da je $|E(\mathbb{F}_q)| \approx q + 1$. Preciznu informaciju o redu grupe $E(\mathbb{F}_q)$ daje Hasseov teorem.

Teorem 1.2.4 (Hasse)**.** *Neka je $\mathbb{F}_q$ konačno polje s q elemenata i $E = E(\mathbb{F}_q)$ eliptička krivulja nad $\mathbb{F}_q$. Tada je*

$$q + 1 - 2\sqrt{q} \leq |E(\mathbb{F}_q)| \leq q + 1 + 2\sqrt{q} \tag{1.28}$$

Drugim riječima, za proizvoljnu eliptičku krivulju E nad $\mathbb{F}_q$ je $|E(\mathbb{F}_q)| = q + 1 - t$, pri čemu je $|t| \leq 2\sqrt{q}$. Broj $t = q + 1 - |E(\mathbb{F}_q)|$ naziva se *Frobeniusov trag* eliptičke krivulje E. Problem izračunavanja reda grupe E tada postaje problem izračunavanja Frobeniusovog traga eliptičke krivulje E na čijoj se osnovi definiraju anomalne i supersingularne krivulje.

Definicija 1.2.5. *Za eliptičku krivulju $E(\mathbb{F}_q)$ nad konačnim poljem $\mathbb{F}_q$ kažemo da je **anomalna** ako je njen Frobeniusov trag $t = 1$, tj. ako je*

$$|E(\mathbb{F}_q)| = q \tag{1.29}$$

Definicija 1.2.6. *Za eliptičku krivulju $E(\mathbb{F}_q)$ nad konačnim poljem $\mathbb{F}_q$, gdje je $q = p^k$, kažemo da je **supersingularna** ako karakteristika polja p dijeli Frobeniusov trag t krivulje $E(\mathbb{F}_q)$.*

Valja spomenuti da vrijedi i obrat Hasseovog teorema (Deuringov teorem) koji kaže da za svaki prirodan broj

$$m \in \langle p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p} \rangle \tag{1.30}$$

postoji eliptička krivulja nad $\mathbb{F}_q$, takva da je $|E(\mathbb{F}_q)| = m$.

U primjenama eliptičkih krivulja često biramo eliptičke krivulje čiji red ima neko zadano aritmetičko svojstvo (prost, ima samo male proste faktore i slično). Vrlo važna činjenica , dokazana od H.W.Lenstra [8], tvrdi da su redovi $|E(\mathbb{F}_q)|$, za $(a, b) \in \mathbb{F}_p \times \mathbb{F}_q$ "skoro uniformno" distribuirani unutar intervala $\langle p + 1 - \sqrt{p}, p + 1 + \sqrt{p} \rangle$ (centralne polovice Hasseovog intervala). To znači da će red slučajno odabrane eliptičke krivulje nad $\mathbb{F}_q$ imati zadano svojstvo s približno istom vjerojatnošću kao i slučajno odabran prirodan broj reda veličine kao p.

O strukturi grupe $E(\mathbb{F}_q)$ nam govori sljedeći teorem.

Teorem 1.2.7. *Neka je E eliptička krivulja nad $\mathbb{F}_q$. Tada je*

$$E(\mathbb{F}_q) \approx \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \tag{1.31}$$

gdje su n_1 i n_2 prirodni brojevi i vrijedi $n_1 | n_2$ i $n_1 | q - 1$.

Ukoliko je $n_1 = 1$, onda je $E(\mathbb{F}_q)$ ciklička grupa. Iz uvjeta $n_1 | nzd(n_1, q - 1)$, zaključujemo da se očekuje da je n_1 mali prirodan broj, a grupa $E(\mathbb{F}_q)$ "skoro ciklička".

Poglavlje 2

Izogenije i graf izogenija

Sad kad smo definirali eliptičke krivulje, zanimaju nas preslikavanja među istima koja bi čuvala njihovu strukturu.

2.1 Izogenije

Definicija 2.1.1. *Neka su E_1, E_2 dvije (ne nužno ravninske*[1]*) algebarske krivulje nad poljem $\mathbb{K}$. Kažemo da je $\phi : E_1 \to E_2$* ***racionalno preslikavanje*** *ako je definirano racionalnim funkcijama $\phi = (u, v), u, v \in \mathbb{K}(E_1)$, takvo da u i v nisu oboje 0, tj. $\phi(P) = (u(P), v(P))$ za $P \in E(\mathbb{K})$. Kažemo da je ϕ* ***morfizam*** *ako je definirana na cijeloj E_1 (ili se može proširiti).*

Definicija 2.1.2. *Neka su E_1 i E_2 eliptičke krivulje.* ***Izogenija*** *s E_1 na E_2 je morfizam $\phi : E_1 \to E_2$ takav da je $\phi(O_1) = O_2$. Dvije eliptičke krivulje E_1 i E_2 su* ***izogene*** *ako postoji izogenija ϕ s E_1 na E_2 takva da je $\phi(E_1) \neq 0$, odnosno ako je ϕ netrivijalna.*

Propozicija 2.1.3 ([6], Teorem 4.8, Poglavlje III)**.** *Svaka izogenija je homomorfizam grupa*[2].

Primjer 2.1.4. *Za svaki $m \geq 1$, množenje s m na eliptičkoj krivulji je izogenija. Za svaki $m \in \mathbb{Z}$ možemo definirati izogeniju množenja s m, $[m] : E \to E$. Za $m > 0$ definiramo na prirodan način :*

$$[m]P = P + P + ... + P, \qquad P \in E \tag{2.1}$$

[1] skup neprekinuto povezanih točaka (jednodimenzionalni skup) koje leže u istoj ravnini

[2] Neka su $(G, \cdot), (H, *)$ grupe. Preslikavanje $f : G \to H$ je homomorfizam grupa ako za sve $a, b \in G$ vrijedi

$$f(a \cdot b) = f(a) * f(b)$$

dok za $m < 0$ definiramo $[m]P = [-m](-P)$. Za $m = 0$ definiramo nul-izogeniju. Da je $[m]$ morfizam slijedi induktivno iz formula za zbrajanje točaka na eliptičkoj krivulji, a očito je $[m]O = O$, pa je $[m]$ izogenija.

Za eliptičku krivulju $E(\mathbb{K})$ i $n \in \mathbb{N}$, ako postoji $\mathbb{K}$-racionalna izogenija $\phi : E \to E'$ takva da je Ker (ϕ) ciklička grupa reda n, kažemo da E ima n-izogeniju.

Definicija 2.1.5. *Neka je $\phi : E_1 \to E_2$ izogenija stupnja m. Tada postoji jedinstvena izogenija $\widehat{\phi} : E_2 \to E_1$ takva da vrijedi*

$$\widehat{\phi} \circ \phi = [m] \tag{2.2}$$

*$\widehat{\phi}$ zovemo **dualna izogenija** od ϕ.*

Lako je zaključiti da je "biti izogen" relacija ekvivalencije na eliptičkim krivuljama.

Razlika izomorfizma i izogenija

U poglavlju (2) definirali smo kada su dvije eliptičke krivulje izomorfne (1.1.3). Izomorfizam je definiran kao morfizam koji je bijekcija, čiju smo definiciju također naveli. Sada nas zanima razlika između izomorfizama i izogenija. Izogenije su homomorfizmi grupa, ali ne i izomorfizmi. Po definiciji, kompozicija izomorfizma i inverza izomorfizma daje preslikavanje identiteta. S izogenijama to nije slučaj. Točnije, ne postoji inverz izogenija koji u kompoziciji s izogenijom daje preslikavanje identiteta. Svaka izogenija ima jedinstvenu dualnu izogeniju koju smo u (2.1.5) definirali. No, kompozicija izogenije i dualne izogenije ima jednostavan oblik - množenje s cijelim brojem m kojeg zovemo stupanj izogenije, gdje "množenje" znači opetovano zbrajanje grupe.

Primjer 2.1.6.

$$\varphi : (x, y) \to \left(\frac{x^2 + 301x + 527}{x + 301}, \frac{yx^2 + 602yx + 1942y}{x^2 + 602x + 466}\right) \tag{2.3}$$

je izogenija stupnja 2 između eliptičkih krivulja E_1 i E_2 jednadžbi

$$\begin{aligned} E_1 &: y^2 = x^3 + 1132x + 278 \\ E_2 &: y^2 = x^3 + 500x + 1005 \end{aligned} \tag{2.4}$$

nad končanim poljem $\mathbb{F}_{2003}$.

Eliptičke krivulje nisu izomorfne jer je grupa $E_1(\mathbb{F}_{2003})$ ciklična, dok $E_2(\mathbb{F}_{2003})$ nije. Postoji teorem koji tvrdi da su dvije eliptičke krivulje nad konačnim poljem izogene ako i samo ako imaju isti broj točaka [5]. Grubi pristup za pokazati izogenost krivulja bio bi računanje broja točaka i uspoređivanje istih (ako dobijemo isti rezultat, krivulje su izogene). Schoofovim algoritmom pokazuje se da obje krivulje imaju 1956 točaka.

2.2 Grafovi izogenija eliptičkih krivulja nad konačnim poljem

Podsjetimo se osnovnih koncepata teorije grafova. Ovdje ćemo se bazirati na neusmjereni graf. Neusmjereni graf G definiramo kao par (V, E) gdje je V konačni skup vrhova i $E \subseteq V \times V$ skup neuređenih parova zvanih bridovi. Kažemo da su vrhovi v, v' povezani bridom, ili incidentni tom bridu, ako je $\{v, v'\} \in E$. Vrhove povezane bridom s vrhom v zovemo susjedni vrhovi vrha v. Šetnja u grafu G je niz $W := v_0 e_1 v_1 e_2 ... e_k v_k$ čiji su članovi naizmjenice vrhovi v_i i bridovi e_i, takvi da su krajevi brida e_i vrhovi $v_{i-1} i v_i$. Ako su svi bridovi u šetnji Ww različiti, kažemo da je W staza. Ako su na stazi svih vrhovi $v_0, ...v_k$ različiti, ona se zove put. Udaljenost $d(v, v')$ dva vrha v, v' je dužina najkraćeg (v, v')-puta u G. Ako v i v' nisu povezani, kažemo da imaju beskonačnu udaljenost. Graf je povezan ako su svaka njegova dva vrha povezana nekim putem. Stupanj vrha v u grafu G predstavlja broj bridova koji su incidentni s v.

Definicija 2.2.1. *Graf izogenija je graf čiji su vrhovi j-invarijante izogenih krivulja, a bridovi izogenije među njima.*

Teorem koji govori o dualnim izogenijama garantira da za svaku izogeniju $E \to E'$ postoji odgovarajuća izogenija $E' \to E$ istog stupnja. Zato, graf izogenije crtamo kao neusmjeren graf.

Graf izogenija supersingularnih eliptičkih krivulja

Neka je p velik prost broj, l prost broj i E_S supersingularne eliptičke krivulje definiranih na konačnom polju $\mathbb{F}_{p^2}$. Vrhovi grafa izogenija supersingulnih eliptičkih krivulja su upravo te krivulje (točnije njihove j-invarijante), dok su bridovi izogenija stupnja l između dvije krivulje.

U teoriji grafova, regularan graf definira se kao graf kojem svaki vrh ima jednak broj susjednih vrhova. Regularan graf s vrhom stupnja k naziva se k-regularan graf ili regularan graf stupnja k. Grafovi izogenija supersingularnih krivulja su $l + 1$-regularni grafovi, što znači da svaki vrh ima točno $l + 1$ susjeda.

Poglavlje 3

Supersingular isogeny Diffie-Hellman protokol

3.1 Povijest SIDH protokola

Godine 1976. Whitfield Diffie i Martin Hellman u znanstvenom su radu *„New directions in cryptography"* objavili metodu za javnu razmjenu tajnih ključeva koja je kasnije postala poznata kao Diffie-Hellmanov protokol za razmjenu ključeva. Budući da se protokol zasniva na potenciranju velikih prostih brojeva, popularnost i praktičnost je stekao tek razvojem dovoljno snažnih računala. Pojavom jakih računala, u svom radu u radu *„Public-Key Cryptosystem Based on Isogenies"* Stolbunov zajedno s Rostovstev-om predlaže kriptosistem sličan Diffie-Hellman-ovom, temeljen na težini izračunavanja izogenija između običnih (ne supersignularnih) eliptičkih krivulja.

Krajem 2010. godine Childs, Jao i Soukharev dolaze do kvantnog algoritma koji izračunava izogenije između običnih (ne supersignularnih) krivulja u subeskponencijalnom vremenu, uz pretpostavku GRH[1]. 2014. Luca De Feo, David Jao i Jerome Plut[7] predstavljaju SIDH, temeljen na težini izračunavanja izogenija između supersingularnih eliptičkih krivulja. Preciznije, postavljaju sljedeći problem :

Definicija 3.1.1 (Supersingularni problem izogenija)**.** *Neka je $\mathbb{K}$ konačno polje i neka su E_1, E_2 dvije supersingularne eliptičke krivulje nad $\mathbb{K}$ takve da $|E_1| = |E_2|$. Izračunajte izogeniju $f : E_1 \to E_2$.*

Prvenstveno, istaknimo neke prednosti u korištenju supersingularnih (a ne običnih) eliptičkih krivulja :

[1] Generalized Riemann Hypothesis

- Rostovstev-Stolbunov protokol ranjiv je na subeksponencijalni napad (Childs-Jao-Soukharev) stoga je teško postići kvantnu sigurnost. Na razinama sigurnosti gdje se može usporediti sa SIDH algoritmom, Rostovstev-Stolbunov protokol puno je sporiji.
- Prednost supersingualrnih krivulja je jednostavnost kontroliranja strukture njihove grupe. Ta činjenica olakšava dobivanje racionalnih torzijskih točaka.
- Jedan od razloga zašto se Child-Jao-Soukharev napad ne može primjeniti na SIDH algoritam je činjenica da je prsten endomorfizama supersingularnih krivulja veći i nije komutativan.

3.2 SIDH protokol

Prije samog algoritma, uvest ćemo pojmove kvocijentnih grupa i generatora grupe potrebne za daljne definicije.

Definicija 3.2.1. *Neka je H podgrupa grupe G. Tada promatramo kvocijentni skup G/H*

$$G/H = \{[x] : x \in G\} \tag{3.1}$$

čiji elementi su lijeve klase[2]

Ako je kvocijentni skup G/N ima strukturu grupe, tada G/N zovemo kvocijentna grupa od G po N.

Definicija 3.2.2. *Neka je G grupa i $S \subseteq G$ proizvoljan podskupo. Tada je*

$$\langle S \rangle := \bigcap_{H \leq G;\ S \subseteq H} H \tag{3.2}$$

podgrupa od G za koju kažemo da je generirana podskupom S i elemente skupa S zovemo generatorima. Ako je S konačan skup i $G = \langle S \rangle$ kažemo da je G konačnogenerirana grupa.

Razmjena ključeva

Da bi tajno komunicirali, Alice i Bob žele izračunati zajednički ključ. Počinju s javnom (oboma vidljivom) supersingularnom eliptičkom krivuljom i završavaju na istoj izogenoj

[2]Neka je G grupa, H neka njezina podgrupa. Tada za svaki $g \in G \setminus H$ skupovi H i $gH = \{gh : h \in H\}$ imaju isti broj elemenata, tj $f : H \to gH, f(h) = gh$ je bijekcija. Skupove $gH, g \in G$ nazivamo lijevim klasama.

krivulji uz različite šetnje na grafu izogenija. Svaka supersingularna eliptička krivulja karakteristike p definirana je na polju $\mathbb{F}_p$ ili $\mathbb{F}_{p^2}$, stoga je dovoljno definirati $\mathbb{F}_q = \mathbb{F}_{p^2}$ kao polje definicije SIDH algoritma.

Fiksiramo male proste brojeve l_A, l_B takve da $l_A \neq l_B$, cijele brojeve e_A, e_B i biramo broj f takav da je $p = l_A^{e_A} l_B^{e_B} f \pm 1$ prost broj. Također, fiksiramo supersingularnu krivulju E nad definiranim poljem $\mathbb{F}_q = \mathbb{F}_{p^2}$.

Alice bira točke $\{P_A, Q_A\} \in E[l_A^{e_A}]$, Bob bira $\{P_B, Q_B\} \in E[l_B^{e_B}]$. Nadalje, Alice bira $\alpha_1, \alpha_2 \in \mathbb{Z}/l_A^{e_A}\mathbb{Z}$ gdje nisu oba broja (α_1, α_2) djeljiva s l_A te računa $K_A = \langle \alpha_1 P_A + \alpha_2 Q_A \rangle$ i izogeniju $a : E \to E_a$, gdje je $E_a = E/\langle K_A \rangle$. Analogno, Bob bira $\beta_1, \beta_2 \in \mathbb{Z}/l_B^{e_B}\mathbb{Z}$ gdje nisu oba broja (β_1, β_2) djeljiva s l_B te računa $K_B = \langle \beta_1 P_B + \beta_2 Q_B \rangle$ i izogeniju $b : E \to E_b$, gdje je $E_b = E/\langle K_B \rangle$.

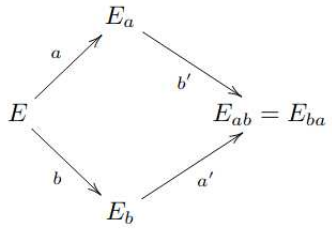
Alice i Bob žele pronaći istu izogenu krivulju prema E, čija će j-invarijanta biti njihov zajednički tajni ključ. Alice računa E_{ab} :

$$E_{ab} = E_b/\langle [\alpha_1]b(P_A) + [\alpha_2]b(Q_A) \rangle \tag{3.3}$$

dok Bob računa E_{ba} :

$$E_{ba} = E_a/\langle [\beta_1]a(P_B) + [\beta_2]a(Q_B) \rangle \tag{3.4}$$

Sljedeći graf predstavlja izračunate izogenije od Alice i Boba-a u procesu traženja zajedničkog tajnog ključa.



Propozicija 3.2.3. *Za E_{ab} i E_{ba} definirane u* (3.3) *i* (3.4) *vrijedi*

$$E_{ab} \cong E_{ba} \tag{3.5}$$

Zbog boljeg razumijevanja daljnih poglavlja prikažimo u kratkim crtama korake cijelog postupka pri implementiranju SIDH algoritma.

1. **Javni parametar**
   Jedna od strana (Alice ili Bob) bira i objavi (veliki) prosti broj p forme $l_A^{e_A} l_B^{e_B} f \pm 1$ t.d. $l_A \neq l_B$ i supersingularnu eliptičku krivulju E nad poljem $\mathbb{F}_p$.

2. **Privatni parametri i računanja**

Alice	Bob
Računa točke $\{P_A, Q_A\} \in E[l_A^{e_A}]$	Računa točke $\{P_B, Q_B\} \in E[l_B^{e_B}]$
Bira tajne cijele brojeve n_A, m_A	Bira tajne cijele brojeve n_B, m_B
Računa izogeniju $a : E \to E_a$	Računa izogeniju $b : E \to E_b$
s jezgrom $K_A = \langle n_A P_A + m_A Q_A \rangle$	s jezgrom $K_B = \langle n_B P_B + m_B Q_B \rangle$
Računa $a(P_B), a(Q_B)$	Računa $b(P_A), b(Q_A)$

3. **Javna razmjena vrijednosti**

Alice	Bob
Šalje Bobu $E_a, a(P_B), a(Q_B)$	Šalje Alice $E_b, b(P_A), b(Q_A)$

4. **Daljna privatna izračunavanja**

Alice	Bob
Računa izogeniju $a' : E_b \to E_{ab}$	Računa izogeniju $b' : E_a \to E_{ba}$
s jezgrom $\langle [n_A]b(P_A) + [m_A]b(Q_A) \rangle$	s jezgrom $\langle [n_B]a(P_B) + [m_B]a(Q_B) \rangle$

5. **Zajednički tajni ključ** je

$$E_{ab} = E/\{K_B, b(K_A)\} = E/\{K_B, K_A\} = E/\{a(K_B), K_A\} = E_{ba}. \tag{3.6}$$

Računanje izogenija i izogenih krivulja

Neka je $\mathbb{F}_q$ polje karakteristike veće od 3, E_1, E_2 dvije eliptičke krivulje definirane kratkim Weierstrassovim jednadžbama (1.10) i $f : E_1 \to E_2$ izogenija. Tada f možemo prikazati kao

$$f(x, y) = (R_1(x, y), R_2(x, y)) \tag{3.7}$$

gdje su R_1, R_2 racionalne funkcije [3].

Velu-ova formula Kako bi razmijenili poruke koristeći SIDH algoritam, Alice i Bob bi trebali moći, uz danu eliptičku krivulju, izračunati joj izogene eliptičke krivulje. To računaju koristeći Velu-ovu formulu.

Teorem 3.2.4 (Velu-ova formula)**.** *Neka je* $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ *eliptička krivulja i* $G(x, y) = x^3 + a_2x^2 + a_4x + a_6 - y^2 - a_1xy - a_3y$. *Neka je* F *konačna podgrupa od* E *i neka su* X, Y *funkcije gdje za svaki* $P \in E$ *vrijedi :*

$$\begin{aligned} X(P) &= x(P) + \sum_{Q \in F - 0} [x(P + Q) - x(Q)] \\ Y(P) &= y(P) + \sum_{Q \in F - 0} [y(P + Q) - y(Q)] \end{aligned} \tag{3.8}$$

[3] Racionalna funkcija zadana je formulom $f(x) = \frac{P(x)}{Q(x)}$, gdje su P i Q polinomi nad $\mathbb{R}$.

Za daljnje razumijevanje, moramo uvesti pojam m-torzije.

Definicija 3.2.5. *Neka je E eliptička krivulja nad poljem $\mathbb{K}$. Množenje s m je preslikavanje $m : E \to E$ definirano s $P \mapsto mP$, za svaki $P \in E$.* ***m-torzija*** *od E je podgrupa $E[m]$ takva da*

$$E[m] = Ker(m) = \{P \in E(\overline{\mathbb{K}}) : mP = \mathcal{O}\} \tag{3.9}$$

Torzijska podgrupa $E(\mathbb{K})_{TORS}$ *eliptičke krivulje E nad poljem $\mathbb{K}$ je*

$$E(\mathbb{K})_{TORS} = \bigcup_{m=1}^{\infty} E[m] \tag{3.10}$$

Označimo s F_2 2-torzijske točke skupa $F - \{0\}$. Promatramo podskup $R \in F - \{0\} - F_2$ takav da

- $R \cup (-R) = F - \{0\} - F_2$
- $R \cap (-R) = \emptyset$

Definiramo $S := F_2 \cup R$. Koristeći zakone zbrajanja eliptičkih krivulja, iz gornjih formula dobivaju se sljedeće općenitije formule :

$$\begin{cases} X = x + \sum_{Q \in S} [\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2}] \\ Y = y - \sum_{Q \in S} [u_Q \frac{2y + a_1 x + a_3}{(x - x_Q)^3} + t_Q \frac{a_1(x - x_Q) + y + y_Q}{(x - x_Q)^2} + \frac{a_1 u_Q - G_x(Q) G_y(Q)}{(x - x_Q)^2}] \end{cases} \tag{3.11}$$

gdje je

$$\begin{cases} Q = (x_Q, y_Q) \\ G_x(Q) = \frac{\partial G}{\partial x}(Q) \\ G_y(Q) = \frac{\partial G}{\partial y}(Q) \\ t_Q = \begin{cases} G_x(Q), if Q \in F_2 \\ 2G_x(Q) - a_1 G_y(Q), if Q \notin F_2 \end{cases} \\ u_Q = (G_y(Q))^2 \end{cases}$$

Tada vrijedi sljedeće :

1. Izogenija $f : E \to E/G$ dana je s $(x, y) \mapsto (X, Y)$ gdje su x, y generatori funkcijskog polja od E opisanog iznad.
2. Eliptička krivulja E/G ima jednadžbu

$$Y^2 + A_1 XY + A_3 Y = X^3 + A_2 X^2 + A_4 X + A_6 \tag{3.12}$$

gdje je

$$\begin{aligned} A_1 = a_1, \quad A_2 = a_2, \quad A_3 = a_3, \\ A_4 = a_4 - 5t, \quad A_6 = a_6 - (a_1^2 + 4a_2)t - 7w \end{aligned} \tag{3.13}$$

gdje je $t = \sum_{Q \in S} t_Q$ i $w = \sum_{Q \in S} u_Q + x_Q t_Q$.

Iako su formule (3.11) općenitije od (3.8), učinkovitije je koristiti formule (3.8) u primjenjivanju SIDH algoritma, to jest računanje slike svake točke krivulje E na izogeniji E' bolje je od eksplicitnog računanja jednadžbi izogenija među njima.

Prikladniji izraz Velu-ove formule Velu-ova formula za izogenije između E i E/G jako je korisna i njegov dokaz vrlo delikatan. Korištena je i u Schoof-ovom algoritmu, prvom deterministčkom algoritmu za brojanje točaka na eliptičkoj krivulji nad konačnim poljima. Elkies, u pokušaju poboljšanja Schoofovog algoritma izražava Velu-ove formule na praktičniji, prikladniji način. Pretpostavljajući da je karakteristika polja veća od 3, daje opciju izražavanja eliptičkih krivulja kao kraćih Weierstrassovih jednadžbi (1.10). S obzirom na to da u kriptografiji uvijek promatramo polja s većim karakteristikama, Elkiesov pristup Velu-ovoj formuli možemo iskoristiti i ovdje. Pretpostavimo da je $p \geq 3$. Eliptička krivulja E nad poljem F_{p^n} je izomorfna sljedećoj Weierstrassovoj formi :

$$E : y^2 = f(x) = x^3 + ax + b \tag{3.14}$$

Tada, Velu-ova formula ima sljedeću formu :

$$X = x + \sum_{Q \in G^*} [x - x(Q) - \frac{f'(x)}{x - x(Q)} + \frac{2f(x)}{(x - x(Q))^2}] \tag{3.15}$$

Izogenije od Alice i Boba

Da bi razmijenili ključeve, Alice i Bob moraju izračunati izogeniju s jezgrom određene konačne podgrupe eliptičke krivulje. U nastavku ćemo proces izračuna razraditi detaljnije. Kao što smo opisali, Alice bira $P_A, Q_A \in E[l_A^{e_A}]$, Bob bira $P_B, Q_B \in E[l_B^{e_B}]$ i oboje objavljuju svoje točke. Također, napomenuli smo da l_A, l_B moraju biti (mali) prosti brojevi različiti jedan od drugog. Pretpostavimo $l_A = 2$ i $l_B = 3$. Zbog jednostavnosti, definiramo $n = e_A$ i $m = e_B$. Alice odabire tajne brojeve α_1, α_2 i računa $K_A = \alpha_1 P_A + \alpha_2 Q_A$. Ponovno, zbog jednostavnosti, neka je $T = K_A$. Alice sada želi izračunati izogeniju $a : E \to E_a$, gdje je $E_a = E/\langle T \rangle$ i vrijednosti $a(P_B), a(Q_B)$. Analogno, Bob računa izogeniju b i vrijednosti $b(P_A), b(Q_A)$.

Kako bi Alice i Bob izračunali izogenije a i b, koriste spomenutu Velu-ovu formulu. Izogenija a je stupnja 2^n i zahtijeva $O(2^n)$ vrijeme izvršavanja. S obzirom na to da je n

velik zbog sigurnosnih razloga, računanje izogenije a postaje kompliciranо. Kako bi prevladala tu prepreku, Alice dijeli a u n izogenija a_i, gdje je svaka stupnja 2 i čije je vrijeme izvršavanja $nO(2)$ te vrijedi $a = a_n \circ a_{n-1} \circ ... \circ a_1$.

Pogledajmo sada u koracima kako možemo izračunati izogenije a_i.

1.korak
Računamo $T_1 = 2^{n-1}T \in E$, element reda 2. Izogenija jezgre T_1 je a_1 (reda 2).

Lema 3.2.6. *Element $a_1(T)$ je reda 2^{n-1}.*

Dokaz. Neka je m cijeli broj takav da je $m \cdot a_1(T) = 0$. S obzirom da za svaki cijeli broj l vrijedi $l \cdot a_1(T) = a_1(l \cdot T)$, imamo :

$$ma_1(T) = 0 \iff mT \in \text{Ker}(a_1) \iff mT \in \langle T_1 \rangle \iff mT \in \langle 2^{n-1}T \rangle \iff 2^{n-1} | \, m \tag{3.16}$$

□

2.korak
Neka je $T_2 = 2^{n-1}a_1(T)$ reda 2. Potrebno je izračunati izogeniju a_2 s jezgrom $\langle T_2 \rangle$. Također, potrebno je izračunati i $E_2 = E_1/\langle T_2 \rangle, a_2 \circ a_1(Q_0), a_2 \circ a_1(Q_1), a_2 \circ a_1(T)$.

Lema 3.2.7. *1. $a_2 \circ a_1(T)$ je reda 2^{n-2}*

2. Ker $(a_2 \circ a_1) = \langle 2^{n-2}T \rangle$

Dokaz. $x \in \text{Ker}\ (a_2 \circ a_1) \iff a_2 \circ a_1(x) = 0 \iff a_1(x) \in \text{Ker}\ (a_2) = \langle T_2 \rangle \iff a_1(x) \in 2^{n-2}a_1(T) \iff x \in \langle 2^{n-2}T \rangle$. □

3.korak
$T_3 = 2^{n-3}a_2 \circ a_1(T)$ je 2-torzija. a_3 je izogenija s jezgrom $\langle T_3 \rangle$. Potrebno je izračunati $E_3 = E_2/\langle T_3 \rangle, a_3 \circ a_2 \circ a_1(Q_1), a_3 \circ a_2 \circ a_1(Q_2), a_3 \circ a_2 \circ a_1(T)$.

Lema 3.2.8. *1. $a_3 \circ a_2 \circ a_1(T)$ je reda 2^{n-3}.*

2. Ker$(a_3 \circ a_2 \circ a_1) = \langle 2^{n-3}T \rangle$

Dokaz. Dokaz je sličan dokazu prethodne leme.

. . .

n. korak
$T_n = 2^{n-n}a_{n-1} \circ a_{n-2} \circ ... \circ a_1(T) = a_{n-1} \circ a_{n-2} \circ ... \circ a_1(T)$ je reda 2. a_n je izogenija s jezgrom $\langle T_n \rangle$. Potrebno je izračunati $a_n \circ a_{n-1} \circ ... \circ a_1(Q_1) = a(Q_1)$ i $a_n \circ a_{n-1} \circ ... \circ a_1(Q_2) = a(Q_2)$.

Lema 3.2.9. *1. $a(T) = a_n \circ ... \circ a_2 \circ a_1(T)$ je reda 1.*

2. *Ker* $(a_n \circ ... \circ a_2 \circ a_1) = \langle T \rangle$.

Dokaz. Dokaz je sličan prethodnim dokazima lema.

Traženje baze torzijskih podgrupa

Pri razmjeni ključeva, Alice i Bob moraju naći baze grupa $E[l_A^{e_A}], E[l_B^{e_B}]$. Detalje traženja baza obradit ćemo u ovom poglavlju.

Želimo definirati sparivanje na $E[m]$, gdje je $E[m]$ torzijska podgrupa (3.2.5). Alice i Bob koriste *Weilovo sparivanje* kako bi provjerili nezavisnost odabranih točaka kao kandidata za bazu. U nastavku se bavimo definicijom Weilovog sparivanja.

Prije toga, definirat ćemo divizore na eliptičkoj krivulji.

Definicija 3.2.10. *Neka je E eliptička krivulja. Divizor na E je formalna konačna suma*

$$D = \sum_{P \in E} n_P P, \tag{3.17}$$

gdje je $n_P \in \mathbb{Z}$ *i* $n_P = 0$ *za konačno mnogo točaka* $P \in E$.

Definicija 3.2.11. *Stupanj divizora je preslikavanje*

$$deg : div(E) \to \mathbb{Z}, \quad D = \sum_{P \in E} n_P P \to \sum_{P \in E} n_P$$

Kada pričamo o stupnju divizora, uglavnom pričamo o njegovoj slici.

Neka je E eliptička krivulja nad poljem $\mathbb{K}$ i $T \in E[m]$, gdje je $E[m]$ torzijska podgrupa. Tada postoji funkcija $f \in \overline{\mathbb{K}}(E)$ koja zadovoljava

$$div(f) = m(T) - m(O) \tag{3.18}$$

Neka je $T' \in E$ točka takva da $[m]T' = T$. Tada postoji funkcija $g \in \overline{\mathbb{K}}(E)$ koja zadovoljava

$$div(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} (T' + R) - (R). \tag{3.19}$$

Vidimo da je $div(g)$ glavni divizor, s obzirom da $|E[m]| = m^2$ i $[m^2]T = O$. Nadalje, funkcije $f \circ [m]$ i g^m imaju iste divizore, stoga množenjem f s prikladnom konstantom iz $\overline{\mathbb{K}}^*$, možemo pretpostaviti

$$f \circ [m] = g^m \tag{3.20}$$

Neka je $S \in E[m]$ druga m-torzijska točka. Tada, za svaku točku $X \in E$, vrijedi

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m \tag{3.21}$$

Možemo promatrati funkciju na $X : g(X+S)/g(X)$ koja uzima konačno mnogo vrijednosti, tj. za svaki X postoji primitivni m-ti korijen iz jedinice[4]. Posebno, morfizam

$$E \to \mathbb{P}^1, S \mapsto g(X+S)/g(X) \tag{3.22}$$

nije surjektivan, i zbog toga je konstanta. Sada možemo definirati Weilovo sparivanje.

Definicija 3.2.12 (Weilovo sparivanje)**.** *Neka je μ grupa primitivnih m-tih korijena jedinice.* ***Weilovo sparivanje*** *je preslikavanje*

$$e_m : E[m] \times E[m] \to \mu_m, \quad (S,T) \mapsto g(X+S)/g(X) \tag{3.23}$$

gdje je $X \in E$ svaka točka za koju su funkcije $g(X+S)$ i $g(X)$ definirane i različite od 0*.*

Weilovo sparivanje omogućuje (uz provjeru nezavisnosti) Alice da provjeri jesu li točke koje joj je Bob poslao slike ispravnih točaka pod izogenijom ispravnog stupnja, o čemu nam govori sljedeća propozicija.

Propozicija 3.2.13. *Neka je $f : E \to E'$ izogenija i $P, Q \in E[N]$ za neki cijeli broj N. Tada*

$$e_N(f(P), f(Q)) = e_N(P,Q)^{deg(f)} \tag{3.24}$$

Da bi dokazali ovu propoziciju, moramo kombinirati sljedeće dvije leme :

Lema 3.2.14. *Weilovo sparivanje je bilinearno, to jest*

$$\begin{aligned} e_N(P_1+P_2,Q) &= e_N(P_1,Q)e_N(P_2,Q) \\ e_N(P,Q_1+Q_2) &= e_N(P,Q_1)e_N(P,Q_2) \end{aligned} \tag{3.25}$$

Dokaz.

$$e_N(P_1+P_2,Q) = \frac{g(X+P_1+P_2)}{g(X)} = \frac{g(X+P_1+P_2}{g(X+P_1)}\frac{g(X+P_1)}{g(X)} = e_N(P_2,Q)e_N(P_1,Q). \tag{3.26}$$

□

Lema 3.2.15. *Neka je $\phi : E \to E'$ izogenija eliptičkih krivulja. Tada za sve m-torzijske točke $S \in E(m)$ i $T \in E'(m)$ vrijedi*

$$e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T) \tag{3.27}$$

[4]Korijenom jedinice nazivamo kompleksan broj w takav da je $w^n = 1$, za neki $n > 0$. Za korijen jedinice w definiramo red od w kao najmanji eksponent l takav da je $w^l = 1$. Ako je l red od w, tada se w naziva **primitivni l-ti korijen jedinice**

Dokaz. Znamo da vrijede jednadžbe $div(f) = m(T) - m(O)$ i $f \circ [m] = g^m$. Tada je

$$e_m(\phi Q, T) = \frac{g(X + \phi S)}{g(Q)} \tag{3.28}$$

Biramo funkciju $h \in \overline{\mathbb{K}}(E)$ koja zadovoljava

$$\phi^*((T)) - \phi^*((Q)) = (\hat{\phi}T) - (O) + divh \tag{3.29}$$

Sada promatramo

$$div(\frac{f \circ \phi}{h^m}) = \phi^* div(f) - mdiv(h) = m(\hat{\phi}T) - m(O) \tag{3.30}$$

i

$$(\frac{g \circ \phi}{h \circ [m]})^m = \frac{f \circ [m] \circ \phi}{(h \circ [m])^m} = \frac{f \circ \phi}{h^m} \circ [m] \tag{3.31}$$

Dolazimo do

$$e_m(S, \hat{\phi}T) = \frac{(g \circ \phi / h \circ [m])(X + S)}{(g \circ \phi / h \circ [m])(X)} = \frac{g(\phi X + \phi S)}{g\phi X} \frac{h([m]X)}{h([m]X + [m]S)} = e_m(\phi S, T) \tag{3.32}$$

□

Sada možemo dokazati propoziciju (3.2.13).

Dokaz. Primjenjujemo lemu (3.2.15) gdje je $S = f(P), T = Q$ i $\hat{\phi} = f$. Dobivamo

$$e_m(f(P), f(Q)) = e_m(\hat{f}(f(P)), Q) = e_m([degf]P, Q) = e_m(P, Q)^{[degf]}, \tag{3.33}$$

gdje zadnja jednakost vrijedi zbog leme (3.2.14). □

Dakle, da bi Alice znala više o valjanosti točaka, mora provjeriti vrijedi li jednakost

$$e_{2^n}(b(P_A), b(Q_A)) = e_{2^n}(P_A, Q_A)^{3^m} \tag{3.34}$$

te ako vrijedi, bit će sigurnija da su točke $b(P_A), b(Q_A)$ koje je Bob poslao slike ispravnih točaka.

Da bi našla bazu torzijske podgrupe $E[2^n]$ Alice mora napraviti sljedeće korake :

1. Alice bira slučajnu točku $P \in E(\mathbb{F}_p)$ i množeći je s $(3^m f)^2$ dobiva točku P', gdje je f izražen preko jednadžbe $p = 2^n 3^m f \pm 1$.

2. Točka P' je gotovo sigurno reda 2^n. To se može provjeriti množeći P' s potencijama od 2. Ako red točke P' bude 2^n, postavlja $P_A = P'$. Ako ne dobije željeni rezultat, pokušava s novom točkom P.

3. Drugu točku, Q_A reda 2^n može dobiti na isti način.

4. Treba provjeriti jesu li točke P_A i Q_A međusobno nezavisne. To radi računajući Weilovo sparivanje $e(P_A, Q_A)$ u $E[2^n]$ te ponovno provjerava da je rezultat reda 2^n. Ponovno, ako rezultat ne bude reda 2^n, bira novi Q_A.

Kako bi izračunala jezgru njene izogenije $\langle \alpha_1 P_A + \alpha_2 Q_A \rangle$, Alice može nastaviti s računanjem $[\alpha_1]P_A$ i $[\alpha_2]Q_A$. Međutim, izračunavanje više točaka na eliptičkoj krivulji je poprilično skup (dug) proces. Bolja opcija je korištenje **dupliciraj-i-dodaj(double-and-add)** algoritma. Standardni dodaj-i-zbroji algoritam za računanje umnoška nP izgleda ovako:

Algorithm 1: Dupliciraj-i-dodaj (double-and-add) algoritam

Input: Cijeli broj $n \in \mathbb{Z}$ i točka $P \in E$
Output: Točka $[n]P$

Raspiši binarno proširenje od n

$$n = e_0 + e_1 2 + e_2 2^2 + e_3 2^3 + ... + e_t 2^t,$$

gdje je $e_0, ..., e_t \in \{0, 1\}$ i $e_t = 1$.
Neka je $Q = P$ i $R = \mathbb{O}$, ako je $e_0 = 0$ ili $R = P$ ako je $e_0 = 1$.
for $i = 1, 2, ..., t$ **do**
    $Q = [2]Q$.
    if $e_i = 1$ **then**
        $R = R + Q$.
return R, koji je jednak $[n]P$.

3.3 Sigurnost i složenost SIDH algoritma

Sigurnost SIDH algoritma bazirana je na pojedinim problemima do čijeg je rješenja teško doći. U ovom poglavlju ćemo definirati sve probleme na kojima se sigurnost temelji.

Ponovno imamo iste pretpostavke i definicije, odnosno p je prost broj forme $p = l_A^{e_A} l_B^{e_B} f \pm 1$, E je supersingularna krivulja nad poljem $\mathbb{F}_{p^2}$ i P_A, Q_A, P_B, Q_B su baze torzijskih podgrupa $E[l_A^{e_A}], E[l_B^{e_B}]$.

(1) *Decisional Supersingular Isogeny problem.* Neka su E, E_a dvije supersingularne krivulje nad poljem $\mathbb{F}_{p^2}$. Odlučite je li E_a $l_A^{e_A}$-izogena krivulji E.

(2) *Computational Supersingular Isogeny problem.* Neka je $a : E \to E_a$ izogenija čija je jezgra $\langle [n_A]P_A + [m_A]Q_A \rangle$, gdje su n_A, m_A slučajno odabrani elementi iz $\mathbb{Z}/l_A^{e_A}\mathbb{Z}$i nisu oba djeljiva s l_A. Za danu krivulju E_a i vrijednosti $a(P_B), a(Q_B)$ pronađite generator jezgre $\langle [n_A]P_A + [m_A]Q_A \rangle$.

(3) *Supersingular Computational Diffie-Hellman problem.* Neka je $a : E \to E_a$ izogenija čija je jezgra jednaka $\langle [n_A]P_A + [m_A]Q_A \rangle$ i $b : E \to E_b$ izogenija jezgre $\langle [n_B]P_B + [m_B]Q_B \rangle$ s elementima $n_A, m_A(n_B, m_B)$ slučajno odabranim iz $\mathbb{Z}/l_A^{e_A}\mathbb{Z}(\mathbb{Z}/l_B^{e_B}\mathbb{Z})$ gdje oba elementa nisu djeljiva s $l_A(l_B)$. Za dane krivulje E_A, E_B i točke $a(P_B), a(Q_B), b(P_A), b(Q_A)$ nađite j-invarijantu na $E/\langle [n_A]P_A + [m_A]Q_A, [n_B]P_B + [m_B]Q_B \rangle$.

(4) *Supersingular Decision Diffie-Hellman problem.* Zadan je konačni sortirani red elemenata s vjerojatnošću $1/2$ iz sljedećih dviju distribucija :

- $(E_A, E_B, a(P_B), a(Q_B), b(P_A), b(Q_A), E_{ab})$ gdje je $E_ab \simeq E/\langle [n_A]P_A + [m_A]Q_A, [n_B]P_B + [m_B]Q_B \rangle$,
- $(E_A, E_B, a(P_B), a(Q_B), b(P_A), b(Q_A), E_C)$ gdje je $E_C \simeq E/\langle [n_A^{'}]P_A + [m_A^{'}]Q_A, [n_B^{'}]P_B + [m_B^{'}]Q_B \rangle$, s elementima $n_A^{'}, m_A^{'}(n_B^{'}, m_B^{'})$ slučajno odabranim iz $\mathbb{Z}/l_A^{e_A}\mathbb{Z}(\mathbb{Z}/l_B^{e_B}\mathbb{Z})$ gdje oba elementa nisu djeljiva s $l_A(l_B)$

Odredite iz koje distribucije je konačno sortirani red elemenata.

(5) *Decisional Supersingular Product problem.* Zadana je izogenija $f : E \to E_3$ stupnja $l_A^{e_A}$ i konačno sortirani red elemenata s vjerojatnošću $1/2$ iz sljedeće dvije distribucije :

- $(E_1, E_2, f^{'})$ gdje je produkt $E_1 \times E_2$ slučajno odabran između svih $(l_B^{e_B}, l_B^{e_B})$-izogenih $E \times E_3$ i gdje je $f^{'} : E_1 \to E_2$ izogenija stupnja $l_A^{e_A}$,
- $(E_1, E_2, f^{'})$ gdje je E_1 slučajno odabrana između svih krivulja koje imaju istu kardinalnost kao E i gdje je $f^{'} : E_1 \to E_2$ izogenija stupnja $l_A^{e_A}$.

Odredite iz koje je distribucije konačno sortirani red elemenata.

Spomenimio najosnovniji napad, odnosno pokušaj rješavanja problema *Decisional Supersingular Isogeny problem* (1), takozvani *meet in the midle* napad.

U praksi, najpoznatiji klasični ili kvantni napad za pronalaženje izogenije $E \to E_a$ s postavkama iz SIDH algoritma je u osnovi generički pristup traženja tajne izogenije od Alice : izračunaj i pamti slučajne šetnje dužine $n_A/2$ u grafu l_A-izogenija počevši od E do E_A dok se te dvije šetnje ne susretnu u sredini. Vrijeme izvršavanja algoritma je $O(p^{1/4})$, s

obzirom na to da je stupanj izogenije koju računa Alice aproksimativno $p^{1/2}$. Međutim, cijena memorije pri izvršavanju ovog algoritma je previsoka. Paralelna verzija *van Oorshot-Wiener*-ovog algoritma s teoretski gotovo istom vremenskom složenošću, ali puno boljim vremensko-prostornim kompromisima smatra se najboljim napadom protiv SIDH-a.

Bibliografija

[1] H. Silverman. *The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986*

[2] Erik Thormarker. *Post-Quantum Cryptography: Supersingular Isogeny Diffie-Hellman Key Exchange*. Thesis, Stockholm University, 2017.

[3] David Kohel. *Endomorphism rings of elliptic curves over finite fields*, PhD thesis, University of California, Berkeley, 1996

[4] Kirsten Eisentrager, Sean Hallgren, Kristin Lauter, Travis Morrison and Christophe Petit. *Supersingular Isogeny Graphs and EndomorphismRings: Reductions and Solutions*

[5] Igor E. Shparlinski *Finite Fields:Theory and Computation, The meeting Point of Number Theory, Computer Science, Coding Theory and Cryptography*

[6] J. H. Silverman *The Arithmetic of Elliptic Curves, 2nd Edition. Graduate Texts in Mathematics. Springer, 2009.*

[7] Luca De Feo, David Jao, and Jérôme Plût *Towards quantum-resistant cryptosys-tems from supersingular elliptic curve isogenies.Journal of Mathematical Cryptology,2014*

[8] J. P. Buhler, H. W. Lenstra, Jr., and C. Pomerance *Factoring integers with the number field sieve, in: The development of the number field siev, Berlin, 1993.*

Sažetak

Algoritmi koji se u današnje vrijeme koriste u kriptografiji mogu se razbiti u polinomijalnom vremenu ako (kada) se kvantna računala počnu razvijati za civilne svrhe. Nesigurnost razmjene podataka na kvantnim računalima postala bi vrlo lako jedan od globalnih problema budućnosti. U ovom radu istražen je SIDH algoritam za koji se vjeruje da je kvantno otporan, s obzirom na to da na njega još uvijek nisu pronađeni ozbiljni napadi. Sadrži metodu razmjene ključeva temeljenu na Diffie-Hellmanovoj razmjeni te mu se sigurnost temelji na teškoći rješavanja problema vezanih uz supersingularne eliptičke krivulje.

U prvom poglavlju napravljen je uvod za čitatelja, od osnovne definicije kriptografije do klasičnih i kvantnih algoritama.

Drugo poglavlje daje jasne definicije eliptičke krivulje i njenih osnovnih svojstava. Također, definirano je ponašanje eliptičkih krivulja nad konačnim poljima.

U trećem poglavlju uvodimo pojam izogenije, gdefiniciju grafa izogenije te opis razlike izogenija i izomorfizma.

Četvrto poglavlje bazira se na SIDH protokolu. Od razmjene ključeva do računanja izogenija i traženja baze torzijskih podgrupa. Kako bi potvrdili kvantu otpornost, spomenuti su sigurnost i složenost SIDH algoritma.

Summary

The algorithms used in the present time for cryptographic purposes, can be broken in polynomial time if the development of a quantum computer becomes reality.Insecurity of data exchange on quantum computers would very easily become one of the global the problem of the future. In this master thesis, we are studying an algorithm that is believed to be quantum resistant, since no serious attacks against it have been found yet, and therefore can be used in post-quantum era, if this becomes a reality. It is called SIDH. It is a key exchange method based on Diffie-Hellmankey exchange, with security based on the difficulty of finding isogenies between supersingular elliptic curve.

First chapter is defined as introduction to reader, from basic definition of cryptography to classic algorithms and why we should consider implementing a new ones.

In second chapter one can find what are elliptic curves and how they behave on finite fields.

Third chapter has focus on defining isogeny, isogeny graph and differences between isomorphism and isogeny.

In fourth chapter we are going through steps of SIDH algoritam, from key exchange to finding bases of torsion subgroups. There is subsection about complexity and security of SIDH algorithm.

Životopis

Rođena sam 27. svibnja 1993. u Dubrovniku. Živjela sam i odrastala u Metkoviću, gdje nakon završene Osnovne škole Stjepana Radića, upisujem Gimnaziju Metković, prirodoslovno-matematički smjer. 2012.godine upisujem Prirodoslovno-matematički fakultet u Zagrebu, smjer Matematika. Preddiplomski studij završavam 2018.godine te iste godine upisujem Diplomski studij Primijenjene matematike, na istom fakultetu.

U siječnju 2017.godine počinjem raditi u Zagrebačkoj banci u odjelu Aplikativnog razvoja. Godinu dana kasnije, nastavljam se razvijati na mjestu programerke u tvrtki Serengeti, gdje radim i danas.