Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike

Kriptografija eliptičkih krivulja

Seminarski rad iz kolegija
suvremene teme iz računalne znanosti

Student:
Marin Kovač

Osijek, 2025.

1 | Uvod

Kriptografija eliptičkih krivulja (ECC[1] u nastavku) jedan je od najmoćnijih kriptosustava javnog ključa. Bazirana je na svojstvima algebarske strukture eliptičkih krivulja nad konačnim poljima. Neovisno su je uveli Victor Miller i Neal Koblitz sredinom 1980-ih, ali se počela široko primjenjivati tek oko 2004. godine. ECC i njena primjena proizašla je iz potrebe za zadovoljavanjem zahtjeva moderne kriptografije. Primarna motivacija leži u postizanju superiornih razina sigurnosti u odnosu na tradicionalne kriptosustave poput RSA. To se prevodi u povećanu otpornost na napade grubom silom, te u novije vrijeme otpornost na kvantne napade. Uz to, važno je i poboljšanje učinkovitosti. ECC koristi manje veličine ključeva što rezultira bržim operacijama šifriranja/dešifriranja pa je posebno pogodan u okruženjima s ograničenim resursima (npr. čipovi).

Iako se o eliptičkim krivuljama i prostoru u kojem žive može pisati u beskraj, proći ćemo samo kroz osnovne definicije i ključne teoreme za razumjevanje principa na kojima je ECC zasnovan. Rad je pisan pod pretpostavkom da čitatelji imaju podlogu u kibernetičkoj sigurnosti, odnosno nemaju duboku matematičku podlogu o pojmovima vezanim za eliptičke krivulje te će se na što jednostavnij, ali svejedno formalan način, pokušati definirati i iskazati sve tvrdnje koje prethode metodi.

[1] Elliptic-curve cryptography

2 | Eliptičke krivulje

2.1 Uvodni pojmovi

Kako bi uopče mogli definirati eliptičke krivulje, moramo poznavati neka svojstva elemenata nad kojima je ona definirana. Prisjetimo se u nastavku nekih osnovnih matematičkih pojmova.

2.1.1 Grupa i polje

Definicija 1 (Grupa)**.** *Skup* $\mathbb{G}$ *opremljen s binarnom operacijom* $(\cdot : \mathbb{G} \times \mathbb{G} \to \mathbb{G})$ *je* ***grupa*** *ako zadovoljava sljedeća svojstva:*

1. *Asocijativnost:*
   $\forall a, b, c \in \mathbb{G},\ \ a \cdot (b \cdot c) = (a \cdot b) \cdot c$
2. *Postojanje neutralnog elementa:*
   $\exists e \in \mathbb{G}$ *takav da* $\forall a \in \mathbb{G},\ \ a \cdot e = e \cdot a = a$
3. *Postojanje inverznog elementa:*
   $\forall a \in \mathbb{G},\ \ \exists b \in \mathbb{G}$ *takav da* $a \cdot b = b \cdot a = e,$ *gdje je e neutralni element*

Grupa $\mathbb{G} = (\mathbb{G}, \cdot)$ *je* ***Abelova grupa*** *ako dodatno vrijedi:*

1. *Komutativnost:*
   $\forall a, b \in \mathbb{G},\ \ a \cdot b = b \cdot a$

Definicija 2 (Polje)**.** *Skup* $\mathbb{F}$ *opremljen s dvije binarne operacije, zbrajanje* $(+)$ *i množenje* $(\cdot)$*, zovemo polje ako zadovoljava sljedeća svojstva:*

1. $(\mathbb{F}, +)$ *je Abelova grupa*
2. $(\mathbb{F} \setminus \{0\}, \cdot)$ *je Abelova grupa*
3. *Distributivnost množenja s obzirom na zbrajanje:*
   $\forall a, b, c \in \mathbb{F},\ \ a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Lako se vidi da su skupovi $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ s uobičajenim operacijama zbrajanja i množenja polja. Navedeni primjeri polja su beskonačna polja, dok će nama od važnosti biti polja s konačnim brojem elemenata.

Definicija 3 (Karakteristika polja)**.** *Karakteristika polja* $(char(\mathbb{F}))$ *je najmanji broj* n *takav da*

$$\underbrace{1 + \cdots + 1}_{n \text{ pribrojnika}} = 0$$

gdje su 1 *i* 0 *redom neutralni element za množenje i neutralni element za zbrajanje. Ako takav* n *ne postoji, onda* $char(\mathbb{F}) = 0$*.*

2.1.2 Polinom

Definicija 4 (Polinom)**.** ***Polinom*** *stupnja* n *nad poljem* K *je izraz oblika*

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$$

gdje $a_i \in K$*.*

Definicija 5 (Nultočka polinoma)**.** *Za* $k \in K$ *kažemo da je* ***korijen*** *ili* ***nultočka*** *polinoma* $f(x)$ *ako* $f(k) = 0$*.*

Napomena 1. *Ako je* k *nultočka, tada je* $f(x)$ *djeljiv polinomom* $x - k$*. Ako je* $f(x)$ *djeljiv polinomom* $(x - k)^m$*, ali nije djeljiv polinomom* $(x - k)^{m+1}$*, onda kažemo da je nultočka* k *višestruka nultočka kratnosti* m*.*

Definicija 6 (Diskriminanta polinoma)**.** *Neka je* $f(x)$ *polinom stupnja* n *i nultočkama* $r_1, ..., r_n$*.* ***Diskriminanta*** D *polinoma* $f(x)$ *je*

$$D = \prod_{i \neq j} (r_i - r_j)^2$$

Teorem 2.1.1. *Determinanta polinoma jednaka je* 0 *ako i samo ako* $f(x)$ *ima višestrukih nultočki.*

2.1.3 Projektivna ravnina

Za definiciju eliptičke krivulje potrebno nam je poznavanje i prostora, odnosno ravnine u kojem krivulja živi. Eliptička krivulja je projektivna što znači da živi u projektivnoj ravnini.

Projektivnu ravninu možemo dobiti proširenjem afine[1] ravnine ako napravimo sljedeće;

1. Za svaki skup paralelnih pravaca proglasimo novu točku u kojoj se oni sijeku i nazovemo ju točka u beskonačnosti $(\mathcal{O})$

2. Za skup točaka u beskonačnosti proglasimo novi pravac koji nazivamo pravac u beskonačnosti i prolazi svim točkama u beskonačnosti

[1] (Euklidska ravnina je vrsta afine ravnine)

Važno je primjetiti da se u projektivnoj ravnini, za razliku od afine, bilo koja dva pravca sjeku u točno jednoj točki.

Postoje razne međusobno ekvivalentne formalne definicije projektivne ravnine. Kako će naši iskazi i dokazi većinom biti elementarni, za projektivnu ravninu dat ćemo algebarsku definiciju.

Definicija 7 (Projektivna ravnina)**.** *Projektivna ravnina* $\mathbb{P}^2(K)$ *je kvocijentni skup*[2] *od* $K^3 \setminus \{(0,0,0)\}$ *po relaciji* $\sim$*.* $(x \sim kx, \forall k \in K)$

Napomena 2. *Projektivnu ravninu nad K ćemo označavati s* KP^2

Iz definicije i ranije opisanog proširenja slijedi da se afina ravnina K^2 ugrađuje u projektivnu ravninu KP^2 preko preslikavanja afinih koordinata u homogene:

$$(x, y) \mapsto (x, y, 1)$$

Komplement slike ovog preslikavanja su sve točke oblika $(x, y, 0)$. Upravo te točke su ranije definirane točke $\mathcal{O}$ koje zajedno definiraju pravac u beskonačnosti $(\{k(1,0,0) + m(0,1,0) : k, m \in K\})$ u K^3.

Primjer 1. *Uzmimo neka dva pravca nagiba 0 u beskonačnoj afinoj ravnini. Možemo naslutiti da će se oni u projektivnoj ravnini sjeći u* $(0,1,0)$*. Neka su*

$$u = \{(x, 0) : x \in K\}$$

$$v = \{(x, 1) : x \in K\}$$

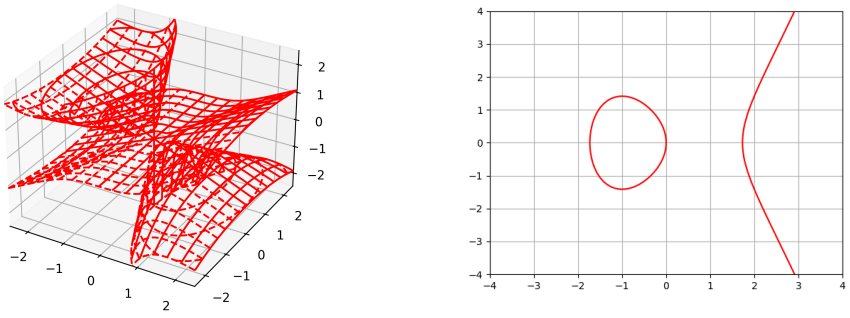
pravci u afinoj ravnini K^2 $(0$ *i* 1 *neutralni elementi pa su u* $K)$*. Preslikavanjem u homogene koordinate dobijamo podskupe od* KP^2*;*

$$\bar{u} = \{(x, 0, 1) : x \in K\}$$

$$\bar{v} = \{(x, 1, 1) : x \in K\}$$

Da bi se u projektivnoj ravnini ovi podskupovi smatrali pravcima, moraju sadržavati točku u beskonačnosti u kojoj se sjeku s ostalim pravcima istog nagiba. Kako je točka projektivne ravnine klasa ekvivalencije omjera koordinata, kretanjem po x u beskonačnost konstante postaju beznačajno male s obzirom na x pa točku $(0, 1, 0)$ *prozivamo točkom u beskonačnosti. To znači da su skupovi* $\bar{u} \cup \{(0,1,0)\}$ *i* $\bar{v} \cup \{(0,1,0)\}$ *pravci u* KP^2 *i sjeku se u točki* $\mathcal{O} = (0,1,0)$*.*

[2] skup klasa ekvivalencije



Slika 2.1: Eliptička krivulja $y^2 = x^3 - x + 5$ u projektivnoj/afinoj ravnini

Napomena 3. *Treba napomenuti da svaka klasa ekvivalencije (x, y, z) ima reprezentant $(x, y, 1)$ pa ćemo u nastavku koristiti koordinate točaka u ravnini unatoč tome što se nalazimo u projektivnom prostoru.*

2.2 Eliptičke krivulje

Definicija 8. *Eliptička krivulja je glatka projektivna krivulja genusa 1 koja ima definiranu točku $\mathcal{O}$.*

Da bi razumijeli ovu definiciju potrebno je znanje algebarske geometrije. Kao što smo već ranije spomenuli, rad je pisan na način da poznavanje takvih karakterizacija nije potrebno. Općenito, eliptička krivulja $E(K)$ je nesingularna krivulja [3] s barem jednom točkom čije točke zadovoljavaju jednadžbu

$$F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \quad (2.1)$$

gdje su $a, b, ..., j \in K$.

Definicija 9. *Za točku (x, y) na krivulji kažemo da je **singularna** ako vrijedi*

$$\frac{\partial F}{\partial x} = \frac{\partial F}{\partial y} = 0$$

Nesingularnost eliptičke krivulje znači da nije singularna ni u jednoj točki, odnosno da komponente od ∇F u točkama koje zadovoljavaju jednadžbu ne iščezavaju istovremeno.

Jednadžba 2.1 ekvivalentna[4] je jednadžbi

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2.2)$$

koju zovemo **generalizirana Weierstrassova forma**. To je forma koja vrijedi za sva polja i koristi se u kriptografij. Međutim, mi ćemo uz dodatne pretpostavke

[3] nema "šiljaka" i ne presjeca se sama sa sobom

[4] dobije se transformacijom

konstruirati kraću formu koja nam je pogodnija za račun. Pretpostavimo onda da je karakteristika polja različita od 2. Kako bi eliminirali xy u jednadžbi 2.2 uvodimo supstituciju $y = y - \frac{a_1x+a_3}{2}$ te ju svodimo na:

$$y^2 = x^3 + b_2x^2 + b_4x + b_6$$

Nadalje, pretpostavimo da karakteristika polja nije 3 pa x^2 možemo eliminirati supstitucijom $x = x - \frac{b_2}{3}$ iz čega slijedi:

$$y^2 = x^3 + c_4x + c_6$$

odnosno

$$y^2 = x^3 + ax + b \tag{2.3}$$

Oblik 2.3 zovemo **kratka Weierstrassova forma**.

Napomena 4. *Kada je karakteristika polja jednaka 2, dijeljenje s 2 nije moguće zato što je to množenje s inverzom od 2, a* $1 + 1 = 0 = 2 \cdot 1$ *i* $2 \cdot x = 0, \forall x \in K$ *pa 2 nema inverz. Analogno vrijedi i za karakteristiku 3.*

Napomena 5. *Navedene supstitucije su izomorfizmi pa te transformacije smijemo raditi. Izomorfizam u kontekstu eliptičkih krivulja znači da krivulje, iako mjenjaju izgled, zadržavaju algebarska i geometrijska svojstva (npr. svojstva zbrajanja se ne mjenjaju).*

U kratkoj Weierstrassovoj formi uvijet nesingularnosti možemo bolje definirati pomoću determinante polinoma s desne strane jednadžbe. Neka je

$$f(x) = x^3 + ax + b \tag{2.4}$$

Teorem 2.2.1. *Eliptička krivulja dana jednadžbom 2.3 je nesingularna ako i samo ako polinom 2.4 nema višestrukih nultočki.*

Dokaz ovog teorema zahtjeva algebarsku geometriju pa ga nećemo dokazivati. Iz teorema 2.1.1 znamo da je tvrdnja da polinom nema višestrukih nultočki ekvivalentna tvrdnji da je determinanta polinoma različita od 0.

Propozicija 1. *Neka je kubni polinom oblika* $f(x) = x^3 + ax + b$*, tada je njegova determinanta*

$$D = -4a^3 - 27b^2$$

Dokaz. Vodeći koeficijent od $f(x)$ je 1, pa dokaz slijedi množenjem izraza

$$(x - r_1)(x - r_2)(x - r_3)$$

i izjednačavanjem/usporedbom s

$$x^3 + ax + b$$

□

Korolar 1. *Krivulja* $y^2 = x^3 + ax + b$ *je nesingularna ako i samo ako je*

$$-4a^3 - 27b^2 \neq 0$$

Dokaz. Slijedi direktno iz 2.2.1 i 1 □

Napomena 6. *Diskriminanta je* 0 *ako i samo ako* $a = -3k^2$ *i* $b = 2k^3$ *za neki* k.

Sada možemo definirati eliptičku krivulju u nama pogodnoj formi.

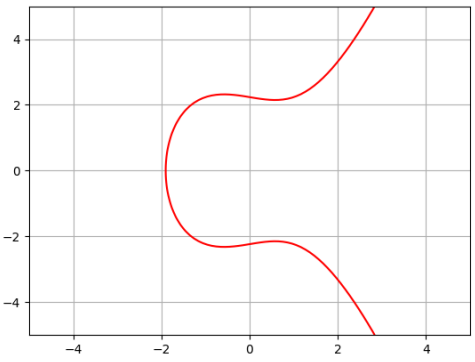
Definicija 10. *Eliptička krivulja* E *nad poljem* K*, karakteristike različite od 2 i 3, je skup točaka* $(x, y) \in K \times K$ *koje zadovoljavaju:*

$$y^2 = x^3 + ax + b$$

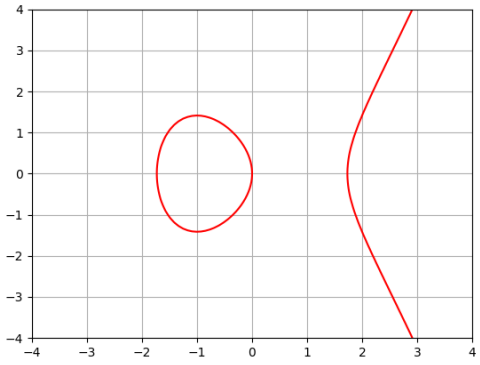
zajedno s točkom u beskonačnosti $\mathcal{O}$*, gdje* $a, b \in K$ *moraju zadovoljavati*

$$4a^3 + 27b^2 \neq 0$$

Napomena 7. *Eliptičku krivulju* E *nad poljem* K *označavat ćemo s* $E(K)$.



Slika 2.2: E_1: $y^2 = x^3 - x + 5$



Slika 2.3: E_2: $y^2 = x^3 - 3x$

Napomena 8. *U homogenim koordinatama jednadžba iz definicije 10 postaje*

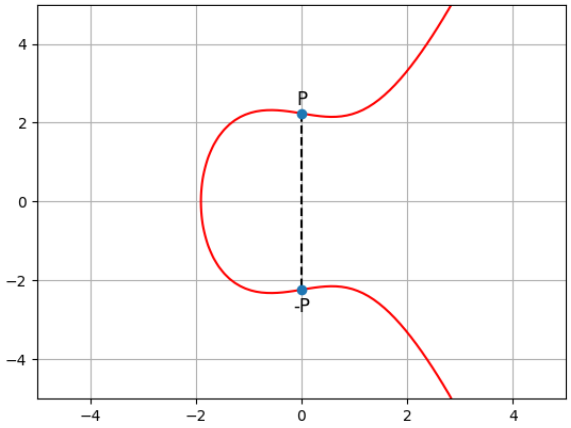
$$zy^2 = x^3 + az^2x + bz^3$$

Presjek ove krivulje s pravcem u beskonačnosti nađemo tako da postavimo $z = 0$ *što implicira* $x^3 = 0$*, odnosno u polju to znači* $x = 0$*. Sve točke oblika* $(0, y, 0)$ *zadovoljavaju jednadžbu, a taj skup je u projektivnoj geometrij točka* $(0, 1, 0)$ *koja je presjek krivulje s pravcem u beskonačnosti.*

2.2.1 Operacije nad eliptičkim krivuljama

U ovom poglavlju pretpostavljamo da je krivulja karakteristike različite od 2 i 3, odnosno koristimo definiciju 10. Također, svi geometrijski prikazi eliptičke krivulje su u $\mathbb{R}^2$. Najvažnije svojstvo eliptičkih krivulja jest da se na njima može uvesti operacija zbrajanja uz koju točke čine Abelovu grupu. To je moguće jer se zbog neprekidnosti krivulje može pokazati da točka u beskonačnosti $\mathcal{O}$ čini neutralni element za zbrajanje.

Svaku operaciju objasnit ćemo geometrijski te uvesti algebarsku definiciju na ravnini. Prva operacija koju ćemo uvesti je unarna operacija $-$. Kako je krivulja simetrična s obzirom na x os, za bilo koju točku P možemo uzeti da $-P$ bude njena osnosimetrična točka.



Definicija 11. *Neka je E eliptička krivulja nad K te $P = (x, y) \in E$. Unarna prefiksna operacija $-$ je funkcija $- : E \mapsto E$ sa sljedećim svojstvima:*

1. *Ako $P = \mathcal{O}$, onda $-P = \mathcal{O}$*
2. *Ako $P \neq \mathcal{O}$, onda $-P = -(x, y) = (x, -y)$*

Napomena 9. *$\mathcal{O}$ leži na xz ravnini iz čega proizlazi prvo svojstvo prethodne definicije.*

Prije definiranja operacije zbrajanja, iskažimo teorem koji će nam biti motivacija za zbrajanje.

Teorem 2.2.2. *Eliptička krivulja sječe pravac u točno 3 točke uzimajući u obzir njihove kratnosti.*

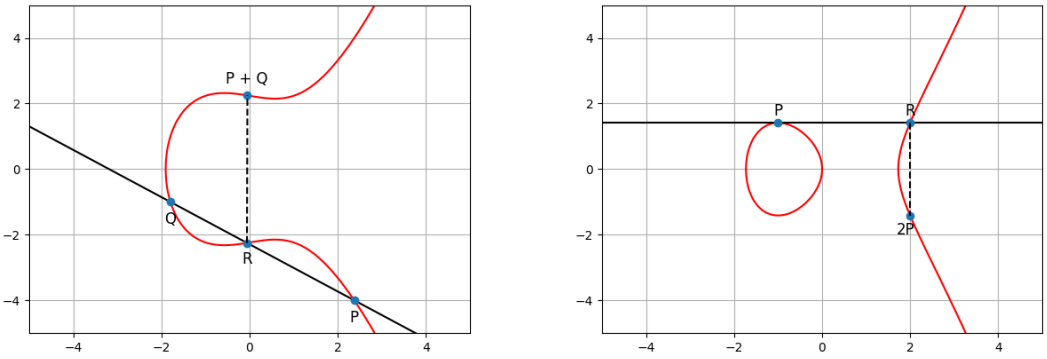
Dokaz. Dokaz uvrštavanjem jednadžbe pravca $y = mx + c$ u jednadžbu krivulje 2.4 i raspisivanjem izraza u polinom trećeg stupnja tvrdnja slijedi iz fundamentalnog teorema algebre. □

Operaciju zbrajanja nad krivuljama uvest ćemo geometrijski. Uzmimo neke točke P i Q koje leže na krivulji. Povućemo li pravac kroz te dvije točke, krivulja sječe jedinstvenu treću točku R. Znamo da treća točka sigurno postoji zbog točke u beskonačnosti $\mathcal{O}$. Za rezultat zbrajanja $P + Q$ uzet ćemo točku $-R$, odnosno osnosimetričnu točku točke R.

U ovakvom zbrajanju imamo par specifičnih slučajeva. Prvi slučaj je pri zbrajanju s točkom $\mathcal{O}$. Tada je ta točka neutralni element i vrijedi $P + \mathcal{O} = P = \mathcal{O} + P$.

Drugi slučaj je kad točku zbrajamo sa samom sobom, odnosno kada je $P = Q$. Tada za pravac koristimo tangentu krivulje u točki P.

Treći slučaj je kad su točke okomite jedna na drugu, odnosno kada je $P = -Q$, tada $P + Q = P - P = \mathcal{O}$.



Napomena 10. *Treba napomenuti da postoji i slučaj kada je točka P točka infleksije. Tada tangenta točke P sjeće krivulju 3 puta u toj točki pa je u tom slučaju $P + P = P$.*

Definirajmo algoritam za zbrajanje točaka na krivulji.

Definicija 12 (Algoritam zbrajanja u $\mathbb{R}^2$)**.** *Neka je $E : y^2 = x^3 + ax + b$ eliptička krivulja te P i Q točke na krivulji.*

1. *Ako $P = \mathcal{O}$, onda $P + Q = Q$*
2. *Analogno za Q*
3. *Inače $P = (x_p, y_p)$ i $Q = (x_q, y_q)$*
4. *Ako $Q = (x_p, -y_p)$, onda $P + Q = \mathcal{O}$*
5. *Inače neka je*

$$\lambda = \begin{cases} \frac{y_q - y_p}{x_q - x_p}, & ako P \neq Q \\ \frac{3x_p^2 + a}{2y_p}, & inače \end{cases}$$

i

$$x_r = \lambda^2 - x_p - x_q$$
$$y_r = \lambda(x_p - x_r) - y_p$$

Tada je $P + Q$ jednak $R = (x_r, y_r)$.

Dokaz. Prve 4 tvrdnje pokazali smo geometrijski. Ako je P različit od Q, onda je λ koeficijent smjera pravca kroz P i Q. Ako je P jednak Q, onda je λ koeficijent smjera tangente kroz P. Iz toga slijedi da je pravac dan jednadžbom $y = \lambda(x - x_p) + y_p$. Neka je $v_p = y_p - \lambda x_p$. Uvrštavanjem jednadžbe pravca $y = \lambda x + v_p$ u jednadžbu krivulje imamo

$$(\lambda x + v_p)^2 = x^3 + ax + b$$

odnosno

$$x^3 - \lambda^2 x^2 + (a - 2\lambda v_p)x + (b - v_p^2) = 0 = (x - x_1)(x - x_2)(x - x_3)$$

BSO neka su $x_1 = x_p$ i $x_2 = x_q$. Množenjem desne strane i promatranjem koeficijenta uz x^2 imamo $-\lambda^2 = -x_p - x_q - x_3$ iz čega slijedi jednadžba od x_r. y_r je osnosimetrična točka nultočke x_3. Kako je ta točka $y = \lambda x_r + v_p$, slijedi $y_r = -y$. □

Kao što je već spomenuto, od velike važnost u teoriji eliptičkih krivulja je da zbrajanje čini Abelovu grupu.

Teorem 2.2.3. *Neka je E eliptička krivulja. Operacija zbrajanja na E je Abelova grupa, odnosno vrijede slijedeća svojstva:*

1. *Asocijativnost:*
   $\forall P, Q, R \in E,\ \ (P + Q) + R = P + (Q + R)$
2. *Postojanje neutralnog elementa:*
   $\forall P \in E,\ \ P + \mathcal{O} = \mathcal{O} + P = \mathcal{O}$
3. *Postojanje inverznog elementa:*
   $\forall P \in E,\ \ P + (-P) = \mathcal{O}$
4. *Komutativnost:*
   $\forall P, Q \in E,\ \ P + Q = Q + P$

Napomena 11. *Operacija zbrajanja je po definicij zatvorena. Zadnja 3 svojstva su definicijska što smo ranije pokazali geometrijski. Dokaz asocijativnosti koristi geometrijsku algebru (npr. [7]) pa teorem nećemo dokazivati.*

2.3 Eliptičke krivulje nad konačnim poljima

Kriptografija eliptičkim krivuljama koristi eliptičke krivulje definirane nad konačnim poljima.

2.3.1 Konačna polja

Definicija 13 (Konačno polje)**.** *Konačno polje je polje s konačnim brojem elemenata i označavat ćemo ga s $\mathbb{F}_q$, gdje je q broj elemenata polja.*

Primjer 2. *Primjer takvog polja je skup cijelih brojeva modulo p koji označavamo s $\mathbb{Z}/pZ$. Lako se pokaže da je takav skup s operacijama zbrajanja i množenja modulo p polje.*

Definicija 14 (Red polja)**.** *Za broj elemenata konačnog polja kažemo da je **red** konačnog polja.*

Polje reda 2 je degenerativno jer sadrži samo 0 i 1 pa ćemo uvijek uzimati da je $q > 2$.

Napomena 12. *Konačno polje se još zove i Galoisovo polje (uz oznaku $GF(q)$).*

Propozicija 2. *Karakteristika konačnog polja mora biti prost broj.*

Dokaz. Pretpostavimo suprotno, odnosno da je n karakteristika koja nije prosta. To znači da n možemo zapisati kao $n = a \cdot b$. Tvrdnja slijedi kontradikcijom zato što polje ne može imati dijeljitelje nule. □

Lema 1. *Ako je p karakteristika polja $\mathbb{F}_q$, onda $\mathbb{F}_q$ sadržava $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

Dokaz. Neka je skup $S = \{0, 1, 1+1, 1+1+1, ..., (p-1)\cdot 1\}$ iz $\mathbb{F}_q$. Lako se pokaže da S zadovoljava sva svojstva polja pa je S potpolje od $\mathbb{F}_q$. Preostaje pokazati da je S izomorfizam u $\mathbb{Z}/p\mathbb{Z}$. Izomorfizam je dan preslikavanjem $\phi : \mathbb{Z}/p\mathbb{Z} \mapsto S$ definiranim s $\phi(a) = 1 \cdot a$. Ovo je očito homomorfizam i po konstrukcij je surjekcija. Preslikavanje je injekcija jer ako $a \cdot 1 = b \cdot 1$, onda $(a-b)\cdot 1 = 0$ što implicira da $a \equiv b \pmod{p}$ zato što p najmanji broj takav da $p \cdot 1 = 0$. S je potpolje od $\mathbb{F}_q$ i izomorfizam u $\mathbb{Z}/p\mathbb{Z}$ što znači da $\mathbb{F}_q$ sadržava $\mathbb{F}_p$. □

$\mathbb{F}_q$ sadrži potpolje $\mathbb{F}_p$ pa je $\mathbb{F}_q$ vektorski prostor nad $\mathbb{F}_p$. Recimo da $\mathbb{F}_q$ ima dimenziju k i neka ima neku bazu $\{v_1, ..., v_k\}$. Svaki elementu $\mathbb{F}_q$ se može iskazat pomoću linearne kombinacije vektora baze gdje su koeficijenti elementi iz $\mathbb{F}_p$. Kako svaki koeficijent može biti jedan od p elemenata iz $\mathbb{F}_p$, slijedi da postoji p^k linearnih kombinacija.

Korolar 2. *Konačno polje reda q postoji onda i samo onda ako $q = p^k$ gdje je p prost broj i $k \in \mathbb{Z}$.*

Napomena 13. *Uočimo da za svaku potenciju prostog broja $q = p^k$ postoji jedinstveno (do na izomorfizam) polje s p elemenata.*

Iz prijašnjih tvrdnji slijedi da ukoliko $q = p^k$, onda postoji $\mathbb{F}_q$ čija je jedna od realizacija $\mathbb{Z}_p/f(x)$ gdje je $f(x)$ ireducibilni[5] polinom stupnja k nad $\mathbb{Z}_p$. Elementi takvog polja su polinomi nad $\mathbb{Z}_p$ stupnja manjeg ili jednakog $k-1$.

Napomena 14. *Zbrajanje i množenje vrše se uz proizvoljan $f(x)$ pa postoje pravila konstrukcije ireducibilnog polinoma uz koje operacije postaju puno efikasnije.*

Uzmemo li $\mathbb{F}_{2^m}$ kao jedno takvo polje te $f(x)$ ireducibilni polinom stupnja m nad $\mathbb{F}_2$, element tog polja možemo reprezentirati nizom od m bitova. Iz toga je jasno zašto su nam polja oblika $\mathbb{F}_{2^m}$ značajna u primjeni.

Suma dva polinoma $A(x)$ i $B(x)$ iz $\mathbb{F}_{2^m}$ je

$$C(x) = \sum_{i=0}^{m-1} (a_i + b_i)x^i$$

gdje se zbrajanje koeficijenata a_i i b_i vrši modulo 2. Kako je

$$a_i + b_i \equiv a_i - b_i \pmod 2$$

slijedi da je operacija zbrajanja jednaka operacij oduzimanja.

Napomena 15. *Primjetimo da je operacija zbrajanja modulo 2 ekvivalentna operacij XOR[6] ($\oplus$) po komponentama te da ne ovisi o bazi.*

Za razliku od zbrajanja, baza utječe na rezultat množenja. Neka su opet $A(x)$ i $B(x)$ iz $\mathbb{F}_{2^m}$ te

$$C(x) = A(x) \cdot B(x) = \prod_{i=0}^{2m-2} c_i x^i$$

[5] nije djeljiv
[6] ekskluzivno ili

gdje

$$c_o \equiv a_o b_o \ (mod\ 2)$$
$$\vdots$$
$$c_{2m-2} \equiv a_{m-1} b_{m-1} \ (mod\ 2)$$

Vidimo da će množenjem na ovakav način rezultat $C(x)$ biti stupnja većeg od $m-1$ pa operacija kao takva neće biti zatvorena u $\mathbb{F}_{2^m}$ zbog čega se množenje definira slično kao na prostim poljima. Operacija množenja vrši se modulo ireducibilan polinom $f(x)$.

Primjer 3. *Neka su $A(x) = x^3 + x + 1$ i $B(x) = x^2 + x$ polinomi iz F_{2^4}. Zbroj tih polinoma jednak je*

$$C(x) = (1 + 0\ mod\ 2)x^3 + (0 + 1\ mod\ 2)x^2 + (1 + 1\ mod\ 2)x + (1 + 0\ mod\ 2)$$

odnosno

$$C(x) = x^3 + x^2 + 1$$

Polinomi kao bitni nizovi veličine 4 su $A = 1011$ i $B = 0110$. Operacijom XOR $\oplus$ na A i B dobili bi isti rezultat

$$C = 1011 \oplus 0110 = 1101$$

Za množenje ovakvih polinoma dodatno moramo odrediti ireducibilan polinom $f(x) \in \mathbb{F}_{2^4}$ stupnja 4. Uzmimo za $f = 1000$ odnosno $f(x) = x^3$. Umnožak $A(x)$ i $B(x)$ sada je;

$$\begin{aligned} C(x) &\equiv (x^3 + x + 1) \cdot (x^2 + x)\ (mod\ f(x)) \equiv \\ &\equiv x^5 + x^4 + x^3 + (1 + 1\ mod\ 2)x^2 + x\ (mod\ f(x)) \\ &\equiv x^5 + x^4 + x^3 + x\ (mod\ f(x)) \equiv x \end{aligned}$$

Binarnim množenjem uz iznimku da bitove "režemo" na veličinu 4 dolazimo do istog rezultata:

$$1011 \cdot 0110 = 0000 + 10110 + 101100 + 0000000 = 100|0010 = 0010$$

Napomena 16. *Primjetimo da je polje $\mathbb{F}_{2^m}$ karatkeristike 2 pa se jednadžba eliptičke krivulje E nad tim poljem transformira u*

$$y^2 + xy = x^3 + ax + b$$

2.3.2 Krivulje nad $\mathbb{F}_p$

Za eliptičke krivulje nad $\mathbb{F}_p$ vrijedi isti algoritam za zbrajanje, ali se sada operacije zbrajanja i množenja vrše modulo p.

Primjer 4. *Neka je $E(\mathbb{F}_7)$ eliptička krivulja nad poljem $\mathbb{F}_7$. Točke ove krivulje tražimo rješavanjem jednadžbi*

$$y^2 \equiv x^3 + 7x + 5\ (mod\ 7)$$

gdje je $x \in \{0, ..., 6\}$. *Uzmemo li na primjer* $x = 1$ *imamo* $1 + 7 + 5 = 13$ *pa za* $x = 1$ *nema odgovarajuće točke* y *budući da* y^2 *nije kongruentno* 13 *modulo* 7. *Uzmemo li* $x = 5$ *imamo* $125 + 35 + 5 = 165$, *a kako je* $5^2 \equiv 2^2 \equiv 165 \pmod 7$ *za* $x = 5$ *slijedi da su* $(5, 2)$ *i* $(5, 5)$ *točke na eliptičkoj krivulji. Ponovimo li ovaj proces za preostalih* 5 x*-eva pronalazimo da su točke ove krivulje*

$$E(\mathbb{F}_7) = \{\mathcal{O}, (3,2), (3,5), (5,2), (5,5), (6,2), (6,5)\}$$

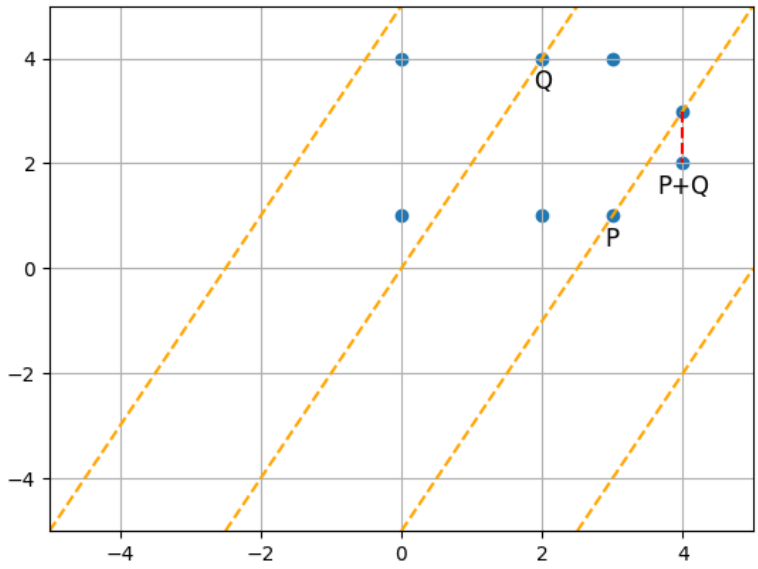
pa je red ove krivulje 7.

Primjer 5. *Neka je* $E(\mathbb{F}_5) = \{\mathcal{O}, (0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)\}$ *eliptička krivulja nad* $\mathbb{F}_5$. *Izračunajmo* $R = P + Q$ *za* $P = (3,1)$ *i* $Q = (2,4)$ *algoritmom za zbrajanje.*

$$\lambda \equiv \frac{4-1}{2-3} \equiv 2 \pmod 5$$

$$x_r \equiv \lambda^2 - x_p - x_q \equiv 4 - 3 - 2 \equiv 4 \pmod 5$$

$$y_r \equiv \lambda(x_p - x_r) - y_p \equiv -2 - 1 \equiv 2 \pmod 5$$



Kako bi napravili kvalitetan izbor krivulje za primjenu, potrebno je poznavanje veličine reda grupe $E(\mathbb{F}_p)$. Svakoj točki x (ima ih p) mogu biti pridružene 2 točke y pa znamo da je maksimalan broj točaka eliptičke krivulje nad poljem p manji od $2p + 2$ ($2p$ točaka i točka u beskonačnosti). Precizniju među od navedene dat ćemo teoremom bez dokaza.

Teorem 2.3.1 (Hasse). *Neka* $\mathbb{F}_p$ *konačno polje s* p *elemenata i* $E(\mathbb{F}_p)$ *eliptička krivulja nad* $\mathbb{F}_p$. *Tada je*

$$p + 1 - 2\sqrt{p} \leq |E(\mathbb{F})| \leq p + 1 + 2\sqrt{p}$$

Napomena 17. *Veličina* $t = p + 1 - |E(\mathbb{F}_p)|$ *naziva se Frobeniusov trag i prema Hasseovom teoremu vrijedi* $t = 2\sqrt{p}$.

Pokazalo se da se za kriptosustave formirane nad eliptičkim krivuljama koje imaju Frobeniusov trag jednak 1, ili ako je karakteristika polja dijelitelj Frobeniusovog traga, mogu kreirati djelotvorni napadi. Problem odabira dobre krivulje je daleko izvan okvira ovog rada.

Postoje deterministički algoritmi za izračun reda krivulje od kojih ćemo neke spomenuti. Jedan takav algoritam je Lang-Trotterova metoda.

Definicija 15 (Legendreov simbol)**.** *Neka je konačno polje* F_p *i* p *neparan prost broj. Legendreov simbol je*

$$\left(\frac{x}{\mathbb{F}_p}\right) = \begin{cases} 1, & \text{ako } t^2 = x, \text{ za neki } t \in \mathbb{F}_p \\ -1, & \text{ako } t^2 = x \text{ nema rješenje} \\ 0, & \text{ako je } x = 0 \end{cases}$$

Teorem 2.3.2. *Neka* $E(\mathbb{F}_p)$ *eliptička krivulja nad konačnim poljem u kratkoj Weierstrassovoj formi. Tada je*

$$\#E(\mathbb{F}_p) = q + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{\mathbb{F}_p}\right)$$

Lang-Trotterov algoritam tvrdi da su tragovi na familiji eliptičkih krivulja "dobro" distribuirani. Vremenska kompleksnost algoritma je $O(pln^2p)$. Postoje algoritmi s boljim kompleksnostima kao što su Shanks-Maestrova metoda i Schoofov algoritam. Schoofov algoritam za dano polje F_p računa točnu vrijednost Frobeniusovog traga u $O(ln^8p)$ bitovnih operacija. Algoritam[7] je kasnije dodatno poboljšan na kompleknost $O(ln^6p)$. Schoofov algoritam radi na način da prvo odredimo skup malih prostih brojeva l takvih da je njihov produkt veći od $4\sqrt{p}$ (po Hasseovom teoremu). Zatim za svaki element skupa l računamo t modulo l. Metoda završava korištenjem kineskog teorema o ostacima rekonstruirajući trag krivulje.

[7] Schoof-Elkies-Atkin

3 | Kriptografija javnog ključa

Definicija 16. *Kriptografija je znanost matematičkih tehnika vezanih uz zaštitu informacija.*

3.1 Uvod

Kriptografija javnog ključa revolucionizirala je sigurnost komunikacije eliminirajući potrebu za unparijednim dogovorom oko tajne. Kriptografija javnog ključa zasniva se na paru ključeva; javnom ključu za enkripciju (šifriranje) i privatnom ključu za dekripciju (dešifriranje). Cilj je pronaći što bolju jednosmjernu funkciju. U tu svrhu radimo eksperiment $\text{Invert}_{\mathcal{A},f}(n)$;

1. Odaberi $x \in \{0,1\}^n$ uniformno i izračunaj $y = f(x)$
2. $\mathcal{A}$ dobija y' i vraća x'
3. Ishod eksperimenta je 1 ako $f(x') = y$, 0 inače

Napomena 18. *Polinomijalno vrijeme izvođenja $\mathcal{A}$ može ovisiti o n, odnosno $\mathcal{A}$ dodatno prima 1^n što zovemo sigurnosni parametar.*

Definicija 17. *Za funkciju $f : \{0,1\}* \mapsto \{0,1\}*$ kažemo da je jednosmjerna ako vrijedi slijedeće:*

1. *Postoji polinomijalan algoritam M_f takav da $M_f(x) = f(x), \forall x$*
2. *Za svaki vjerojatnostni polinomijalan algoritam $\mathcal{A}$, postoji zanemariva $\epsilon(n)$ takva da*

$$P(Invert_{\mathcal{A},f}(n) = 1) \leq \epsilon(n)$$

U kriptografij javnog ključa, ključevi su direktno povezani s jednosmjernim funkcijama. Uz poznavanje javnog ključa, funkcija je jednosmjerna, dok uz poznavanje privatnog ključa funkcija postaje dvosmjerna. Drugi naziv za kriptosustav javnog ključa je **asimetrični kriptosustav**.

Definicija 18. *Asimetrični kriptosustav definiramo kao uređenu petorku $(\mathcal{M}, \mathcal{C}, Gen, Enc, Dec)$ gdje je:*

1. *$\mathcal{M}$ prostor poruka.*
2. *$\mathcal{C}$ prostor šifrata.*

3. *Gen stohastički generator ključeva* $((pk, sk) = Gen)$.

4. $Enc(m, pk)$ *funkcija šifriranja* $(c = Enc(m, pk))$.

5. $Dec(c, sk)$ *funkcija dešifriranja* $(m = Dec(c, sk))$.

Napomena 19. *Generator uobičajeno prima i sigurnosni parametar* 1^n.

Primjer 6 (RSA)**.** *Jedan primjer asimetričnog kriptosustava je RSA* [1] *koji se zasniva na činjenici da je za pozitivne cijele brojeve* e, d, n *takve da*

$$\forall m \in \mathbb{N}, m \leq n \; i \; (m^e)^d \equiv m \; (mod \; n)$$

teško pronaći d *ako znamo* e *i* n*. Neka je* $n = pq$ *gdje su* p *i* q *prosti brojevi te neka su* $\mathcal{M} = \mathcal{C} = \mathbb{Z}_n$*. Nadalje,*

$$Gen = ((n, e), (n, d))$$
$$Enc(m, (n, e)) = m^e \; (mod \; n)$$
$$Dec(c, (n, d)) = c^d \; (mod \; n)$$

gdje su ključevi takvi da vrijedi:

$$n = pq$$
$$gcd(e, \lambda(n)) = 1$$
$$d \cdot e \equiv 1 \; (mod \; \lambda(n))$$
$$\lambda(n) = lcm(p - 1, q - 1)$$

Za primjer uzmimo $p = 61$ *i* $q = 53$*. Iz toga imamo da je* $n = 3233$*. Pomoću euklidovog algoritma računamo da je* $\lambda(n) = 780$*. Sada biramo* e *relativno prost s* 780 *pa neka je* $e = 17$*.* d *izračunamo pomoću* e *i* $\lambda(n)$*. Iz toga imamo da je šifrat* $c = m^{17} \; mod \; 3233$ *i poruka* $m = c^{413} \; mod \; 3233$*.*

Kako bi se osigurala kvalitete kriptosustava uvedeni su sigurnosni modeli kojima se ispituju svojstva sustava. Mi ćemo opisati dva najznačajnija zahtjeva:

Definicija 19 (Zahtjev ispravnosti)**.** *Za asimetrični kriptosustav kažemo da je ispravan ako*

$$\forall m \in \mathcal{M} \; i \; \forall (pk, sk) \; generiran \; pomoću \; Gen \; vrijedi : Dec(Enc(m, pk), sk) = m$$

Teorem 3.1.1 (Fermatov mali teorem)**.** *Neka je* p *prost broj i* a *cijeli broj. Vrijedi*

$$a^p \equiv a \; (mod \; p)$$

Primjer 7. *Provest ćemo zahtjev ispravnosti na RSA. Trebamo pokazati da* $(m^e)^d \equiv m \; (mod \; pq)$*. Kako je* $\lambda(n)$ *dijeljiv s* $p - 1$ *i* $q - 1$*, za* $k, h \in \mathbb{N}$ *imamo* $ed - 1 = h(p - 1) = k(q - 1)$*. Sada ako* $m \equiv 0 \; (mod \; p)$ *onda* $m^{ed} \equiv 0 \; (mod \; p)$*. Inače* $m^{ed} = m^{ed-1}m = m^{h(p-1)}m = (m^{p-1})^h m$ *pa po teoremu 3.1.1 imamo* $(m^{p-1})^h m \equiv m \; (mod \; p)$ *Analogno napravimo i za* $m^{ed} \equiv 0 \; (mod \; q)$*. Iz toga slijedi* $(m^e)^d \equiv m \; (mod \; pq)$*.*

[1] Rivest-Shamir-Adleman

Očito je da sustavi u kojima ne vrijedi zakon ispravnosti nisu od koristi. Od zahtjeva sigurnosti najznačajnij je IND-CPA (indistinguishability under chosen-plaintext attack). IND-CPA definira se igrom izazivača i protivnika. Slijed igre je slijedeći:

1. Izazivač generira par ključeva *sk* i *pk* te šalje ključ *pk* protivniku
2. Protivnik radi proizvoljan polinomijalan broj operacija i nakon toga šalje dva plaintexta M_0 i M_1 izazivaču
3. Izazivač bira nasumičan bit $b \in \{0, 1\}$ i šalje "izazov" $C = Enc(M_b, pk)$ protivniku.
4. Protivnik radi proizvoljan polinomijalan broj operacija i pogađa bit b'

Kriptosustav je siguran ako protivnik ima zanemarivo malu prednost nad slučajnim pogađanjem, odnosno;

Definicija 20 (Zahtjev sigurnosti)**.** *Za asimetrični kriptosustav kažemo da je IND-CPA siguran ako*

$$\forall \mathcal{A},\ \exists \epsilon(n)\ \ t.d.\ \ P(b = b') \leq \frac{1}{2} + \epsilon(n)$$

gdje je $\mathcal{A}$ polinomijalni algoritam napadača, $\epsilon(n)$ zanemariva funkcija te P vjerojatnost pobjede protivnika.

Napomena 20. *Ovu definiciju možemo interpretirati na način da se u sigurnim sustavima ne može dobiti nikakva informacija promatranjem šifrata.*

3.2 Problem diskretnog logaritma

Ne postoji formalan dokaz postojanja jednosmjernih funkcija pa njihovu egzistenciju moramo pretpostavit. Prilikom konstrukcije asimetričnih kriptosustava, odnosno jednosmjernih funkcija, najčešće se uzimaju u obzir teški matematički problemi iz teorije brojeva. Jedan takav problem zove se problem diskretnog logaritma.

Definicija 21. *Neka je $(G, *)$ konačna grupa, $g \in G$ i $H = \{g^i : i \geq 0\}$ podgrupa od G. Neka je $x \in \mathbb{Z}$ najmanji broj (zbog jedinstvenosti) takav da*

$$h = g^x = \underbrace{g + \cdots + g}_{x\ puta}$$

Ako takav x postoji zovemo ga diskretni logaritam i označavamo s $log_g h$.

Može li se generalni diskretni logaritam izračunati u polinomijalnom vremenu neriješen je problem u računalnoj znanosti. To znači da nije otkriven (ne kvantni) algoritam za izračun diskretnog logaritma zbog čega je potenciranje nad konačnim poljem dobar kandidat za jednosmjernu funkcije.

Definicija 22 (Red točke)**.** *Neka je G grupa s neutralnim elementom* 1 *i neka je* $P \in G$*. Za broj n točke P kažemo da je red točke ako je to najmanji broj takav da* $P^n = 1$*.*

Propozicija 3. *Neka je G konačna grupa. Svaki element od G ima konačan red. Ako* $a \in G$ *reda d i k najmanji takav da vrijedi* $a^k = e$*, onda* $d|k$*.*

Primjer 8. *Neka je G multiplikativna grupa od* $E(\mathbb{F}_p)$ *gdje za* $P, Q \in E(\mathbb{F}_p)$ *problem diskretnog algoritma predstavlja određivanje* $d \in [0, n-1]$*, pri čemu je n red točke P, takav da* $Q = nP$*.*

3.2.1 Problem diskretnog logaritma za eliptičke krivulje

Definicija 23 (ECDLP)**.** *Neka je E eliptička krivulja nad* $\mathbb{F}_p$ *i neka su Q i P točke u* $E(\mathbb{F}_p)$*. Problem diskretnog logaritma za eliptičke krivulje je problem pronalaska* $n \in \mathbb{N}$ *takvog da je* $Q = nP = \underbrace{P + \cdots + P}_{n}$*.*

$$n = \log_p(Q)$$

Napomena 21. *n zovemo eliptički diskretni logaritam od Q u odnosu na P.*

Kada su E i P ispravno odabrani, rješavanje diskretnog logaritma smatra se nemogućim uz pretpostavku da je red točke P dovoljno velik da je teško provjeriti sve mogućnosti za d.

Šifriranje u sustavima baziranim na problemu diskretnog logaritma za eliptičke krivulje obavlja se računanjem nP. Kao što smo već napomenuli, želimo da nam je funkcija šifriranja što efikasnija. Prvo primjetimo budući da je $E(\mathbb{F}_p)$ konačan, postoje cijeli brojevi $k > j$ takvi da je $kP = jP$. Tada je po propozicij 3 $(k-j)$ red točke P što znači da je vrijednost $log_P(Q)$ element iz $\mathbb{Z}/(k-j)\mathbb{Z}$. Ukoliko znamo da je $n = n_o + i(k-j)$ jednostavno možemo staviti $log_P(Q) = n_o P$. Važnija stvar za primjetiti je da broj n možemo zapisati u binarnom obliku $n = n_0 + n_1 2 + n_2 2^2 + ... + n_r 2^r$. Tada uz oznaku $P_i = 2^i P$, odnosno $P_i = 2P_{i-1}$ imamo da je $nP = n_0 P_0 + n_1 P_1 + ... + n_r P_r$. Ukupno vrijeme izračuna na ovaj način je najviše $2r$, odnosno množenje smo sveli na logaritamsku kompleksnost $log_2(n)$, što nam omogućava računanje nP za velike vrijednosti n.

Svi sustavi koji u definicij koriste grupu $\mathbb{Z}_p^*$ mogu se modificirati tako da koriste $E(\mathbb{Z}_p)$. Razlika je što budući da je eliptička krivulja aditivna umjesto potenciranja imamo uzastopno zbrajanje.

Napomena 22. *ECDLP puno je teži problem nego diskretni logaritam multiplikativne grupe konačnog polja pa se ista sigurnost postiže za puno manju veličinu ključa.*

U nastavku navest ćemo neke od sustava zasnovane na ECDLP.

3.3 ElGamalov kriptosustav

Originalno, kriptosustav je koristio multiplikativnu grupu $G = (\mathbb{Z}/p\mathbb{Z})*$. Najbrži poznati algoritam za traženje diskretnog logaritma u $(\mathbb{Z}/p\mathbb{Z})*$ je kompleksnosti $e^{O((\log p)^{\frac{1}{3}}(\log\log p)^{\frac{2}{3}})}$ što znači da je po kompleksnosti ekvivalentan problemu

faktorizacije. Modificiranjem problema da koristi grupu $E(\mathbb{F}_p)$ imamo slijedeći sustav:

Definicija 24. ***ElGalmanov kriptosustav ECC*** *eliptičke krivulje $E(\mathbb{F}_p)$ nad konačnim poljem $\mathbb{F}_p$ i točkom $P \in E(\mathbb{F}_p)$ je uređena petorka $(\mathcal{M}, \mathcal{C}, Gen, Enc, Dec)$ takva da:*

$$\begin{aligned} \mathcal{M} &= E(\mathbb{F}_p) \\ \mathcal{C} &= E(\mathbb{F}_p)^2 \\ Gen = (pk, sk) &= (aP, a) \\ Enc(m, pk) &= (kP, m + k\ pk) \\ Dec((c_1, c_2), sk) &= c_2 - sk\ c_1 \end{aligned}$$

gdje su $a, k \in \{1, 2, ..., n-1\}$ nasumično generirani i n red točke P.

Napomena 23. *Lako se vidi da je sustav ispravan. $Dec(c, sk) = c_2 - a\ c_1 = m + k(aP) - a(kP) = m + k(aP) - k(aP) = m$*

Uz doslovno prevođenje sustava $(\mathbb{Z}/p\mathbb{Z})^*$ na $E(\mathbb{F}_p)$ moramo uzeti u obzir i probleme koji se pojavljuju. Primjerice, moramo osmisliti algoritam koji će preslikati naše poruke u skup $\mathcal{M}$, odnosno točke na krivulji. Za to ne postoji deterministički algoritam pa se u ovom slučaju koristi probabilistički algoritam. Primjer jednog takvog algoritma temelji se na činjenici da polovinu svih elemenata čine kvadrati. Neka se otvoreni tekst sastoji od cijelih brojeva između 0 i M. Za cijeli broj m u k koraka tražimo $x = mk + j$ gdje je $j \in \{1, 2, ..., k\}$ minimalan takav da $x^3 + ax + b$ bude kvadrat modulo p. Pokazuje se da je približna vrijednost da u k koraka pronađemo takav x dana s $1 - (\frac{1}{2})^k$ pa za npr. $k = 50$ imamo skoro gotovo siguran pogodak. Formulom $m = \lfloor \frac{x-1}{k} \rfloor$ vraćamo točku u otvoreni tekst.

Napomena 24. *Ovim algoritmom poruka se znatno poveća što je također problematično.*

3.4 Menezes-Vanstoneov kriptosustav

Ovaj kriptosustav je varijanta ElGamalovog kriptosustava. Eliptičke krivulje koriste se za maskiranje, a otvoreni tekstovi i šifrati su uređeni parovi polja koji ne moraju biti točke eliptičke krivulje.

Definicija 25. ***Menezes-Vanstoneov kriptosustav ECC*** *eliptičke krivulje $E(\mathbb{F}_p)$ nad konačnim poljem $\mathbb{F}_p$ i točkom $P \in E(\mathbb{F}_p)$ je uređena petorka $(\mathcal{M}, \mathcal{C}, Gen, Enc, Dec)$ takva da:*

$$\begin{aligned} \mathcal{M} &= (\mathbb{F}_p)^2 \\ \mathcal{C} &= E(\mathbb{F}_p)^2 \\ Gen = (pk, sk) &= (aP, a) \\ Enc(m, pk) &= (kP, (m_1 Q_x, m_2 Q_y)) \\ Dec((c_1, c_2), sk) &= (c_{2_1}/Q_x, c_{2_2}/Q_y) \end{aligned}$$

gdje su $a, k \in \{1, 2, ..., n-1\}$ nasumično generirani za n red točke P, $Q = skc_1 = ac_1 = a(kP)$ i c_{2_1}, c_{2_2} komponente c_2.

U usporedbi s ElGamalovim kriptosustavom, ovaj sustav ima šifru od dvije točke umjesto četiri.

3.5 Diffie-Hellman razmjena ključeva

Kriptosustave koje smo do sada naveli su jednosmjeran način komunikacije u kojem jedna osoba ima privatni ključ, a druga javni. Kako bi mogli imati dvosmjernu sigurnu komunikaciju mora postojati protokol razmjene ključeva. Diffie-Hellman je najpoznatij i najranij praktični primjer javne razmjene ključeva. U kontekstu ovog rada nas specifično zanima eliptički Diffie-Hellman. Pretpostavimo da Alice želi uspostaviti tajni ključ s Bobom, ali je kanal njihove komunikacije javan. Najprije Alice i Bob dogovore se oko parametara (p, a, b, P, n, h) gdje je p prost red polja, a i b parametri krivulje, P bazična točka reda n i kofaktor h koji ćemo mi ignorirati. Također, i Bob i Alice moraju imati svoj privatni ključ d nasumično odabran iz $[1, n-1]$ i javni ključ $Q = dP$. Neka je Alice ključ (d_A, Q_A) i Bobov ključ (d_B, Q_B). Alice računa $(x_k, y_k) = d_A \cdot Q_B$ te Bob računa $(x_k, y_k) = d_B \cdot Q_A$. Sada je x_k njihova zajednička tajna jer vrijedi:

$$d_A \cdot Q_B = d_A \cdot d_B \cdot P = d_B \cdot d_A \cdot P = d_B \cdot Q_A$$

Nakon uspostave zajedničkog tajnog ključa, Alice i Bob mogu komunicirati putem nekog od ranije navedenih kriptosustava.

Primjer 9. (*Primjer iz* [8]) *Alice i Bob žele imati siguran kanal komunikacije te su odabrali koristiti Menezes-Vanstoneov kriptosustav. Za eliptičku krivulju odabrali su* $y^2 = x^3 + x + 1$ *nad poljem* $\mathbb{Z}_{31}$ *te bazičnu točku* $P = (9, 10)$. *Iz toga slijedi da je* $\#\mathbb{Z}_{31} = 34$ *i točka* P *reda* 34. *Točke ove eliptičke krivulje prikazane su tablicom: Poisto-*

k	$k \times P$	k	$k \times P$	k	$k \times P$	k	$k \times P$	k	$k \times P$	k	$k \times P$
1	(9,10)	7	(6,24)	13	(27,10)	19	(5,22)	25	(16,23)	31	(23, 13)
2	(18,29)	8	(24,29)	14	(26,21)	20	(26,10)	26	(24,2)	32	(18, 2)
3	(23,19)	9	(16,8)	15	(5,9)	21	(27,21)	27	(6,7)	33	(9, 21)
4	(4,22)	10	(20,2)	16	(19,3)	22	(28,18)	28	(17,13)	34	$\mathcal{O}$
5	(25,16)	11	(22,22)	17	(10,0)	23	(22,9)	29	(25,15)		
6	(17,18)	12	(28,13)	18	(19,28)	24	(20,29)	30	(4,9)		

vjetimo $a = 1$, $b = 2$, ..., $z = 26$. *Sada komunikaciju provode na slijedeći način:*

1. *Alice odabire tajni ključ* 7 *i računa* $7 \times P = (6, 24)$
2. *Bob odabire tajni ključ* 12 *i računa* $12 \times P = (28, 13)$
3. *Alice želi poslati poruku 'ok', odnosno* $(15, 11)$. *Odabire slučajan* $k = 5$ *te šifrira poruku slijedećim procesom;* $(c_1, c_2) = 5 \times (28, 13) = (24, 29)$, $5 \times P = (25, 16)$ *te* $c_1 x_1 = 24 \cdot 15$ *mod* $31 = 19$ *i* $c_2 x_2 = 29 \cdot 11 \mod 31 = 9$. *Nakon toga šalje poruku* $((25, 16), 19, 9)$.
4. *Nakon što primi poruku, Bob računa* $(c_1, c_2) = 22 \times (25, 16) = (24, 29)$ *zatim invertira elemente 24 i 29 modulo 31 koristeći Euklidov algoritam. Bob sada može očitati originalnu poruku:* $(19 \cdot 22, 9 \cdot 15)$ *mod* $31 = (15, 11)$, *tj. 'ok'.*

4 | Dodatno

4.1 Napadi na diskretni logaritam eliptičke krivulje

Jedna od strategija napada na problem diskretnog logaritma je svođenje problema na jednostavnij problem diskretnog logaritma. To se radi algoritmima koji reduciraju problem diskretnog logaritma za eliptičke krivulje na problem diskretnog logaritma za multiplikativne grupe nad konačnim poljem. Jedan takav napad zove se MOV napad. Radi po principu Weilovog uparivanja koji uzme dvije točke s krivulje i preslika ih u točku konačnog polja. Supersingularne eliptičke krivulje, odnosno eliptičke krivulje za koje vrijedi $a \equiv 0 \ (mod \ p)$ posebno su osjetljive na ovaj napad. Postoji i napad imenom Frey-Ruck koji radi vrlo slično, ali umjesto Weilovog uparivanja koristi Tate-Lichtenbaum uparivanje. Uz to postoje i razni napadi nad općenitim eliptičkim krivuljama kao npr. Baby step/Giant step i Pollardove metode. Puno više o tome možete proučiti u [4].

4.2 Poboljšanje efikasnosti eliptičkih krivulja

Prostornu efikasnost možemo poboljšati drugačijom reprezentacijom točaka. Znamo da su eliptičke krivulje simetrične s obzirom na x os. Broj bitova za reprezentaciju točke na eliptičkoj krivulji možemo za duplo smanjiti primjetimo li da uvijek postoje dvije točke za neki x čija je razlika u y samo predznak. To znači da bilo koju točku $P = (x, y)$ možemo prikazati pomoću x koordinate i bita b.

Računsku efikasnost možemo poboljšati homogenim koordinatama eliminirajući potrebu za računanjem inverza modulo. U projektivnim koordinatama algoritam za zbrajanje je oblika

$$R = \left(\lambda^2 - \frac{x_p}{z_p} - \frac{x_q}{z_q}, \lambda(\frac{x_p}{z_p} - \lambda^2 + \frac{x_p}{z_p} + \frac{x_q}{z_q}) - \frac{y_p}{z_p}, 1\right)$$

gdje se sve operacije vrše modulo p. Kako su homogene koordinate točke klasa ekvivalencije smijemo ih množiti s

$$z_p z_q (x_q z_p - x_p z_q)^3 \neq 0 \ mod \ p$$

pa imamo da je R oblika

$$R = (vw, u(v^2 x_p z_q - w) - v^3 y_p z_q, z_p z_q v^3)$$

gdje izrazi u,v i w ne sadrže inverze.

Literatura

[1] Henry McKean , Victor Moll, *Elliptic curves*

[2] Menezes A. J. , van Oorschot P. C., Vanstone S. A., *Handbook of applied cryptography*

[3] Katz J., Lindell Y., *Introduction to modern cryptography*

[4] Kenneth H. Rosen, *Eliptic curves, Number theory and cryptography, Second edition*

[5] Kokanović A., *Eliptičke krivulje u kriptografiji*, Sveučilište J.J.Strossmayera u Osijeku, Odjel za matematiku

[6] Musulin Z., *Eliptičke krivulje i kriptiranje*, Sveučilište u Zagrebu, PMF

[7] https://building-babylon.net/2024/05/26/associativity-of-the-group-law-on-a-non-singular-elliptic-curve-via-the-cayley-bacharach-theorem/

[8] Dino Sejdinović, *Eliptičke krivulje u kriptografiji*, Osječki matematički list 6, 85-97

[9] https://web.math.pmf.unizg.hr/ duje/ecc/konpolja.html