Zbrajanje i multiplikacija točaka na eliptičkim krivuljama

Badrov, Mladen

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Mladen Badrov

ZBRAJANJE I MULTIPLIKACIJA TOČAKA NA ELIPTIČKIM KRIVULJAMA

Diplomski rad

Voditelj rada:
Akad. Andrej Dujella

Zagreb, rujan, 2014

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. _____

Sadržaj

Uvod

Proučavanje eliptičkih krivulja počinje sredinom devetnaestog stoljeća od strane proučavatelja algebre, algebarske geometrije i teorije brojeva. No prava eksplozija radova je krenula nakon 1984. godine, nakon što je Hendrik Lenstra opisao algoritam za množenje prirodnih brojeva koji se oslanja na svojstva eliptičkih krivulja. Pojačala su se istraživanja drugih primjena eliptičkih krivulja, kao u kriptografiji i računalnoj teoriji brojeva. Između ostalih rezultata, dokazan je i Fermatov posljednji teorem. Jedna od bitnijih primjena za današnje vrijeme je u svakom slučaju kriptografska primjena, u kriptografiji javnog ključa. 1985. godine, Neal Koblitz i Victor Miller su izumili kriptografiju eliptičkih krivulja, do danas jedinu pravu konkurenciju RSA kriptosustavu. Kriptografija eliptičkih krivulja se temelji na problemu diskretnog logaritma na eliptičkim krivuljama. Najbolji poznati algoritmi za riješavanje problema diskretnog logaritma na eliptičkim krivuljama su eksponencijalne složenosti, za razliku od algoritama za faktorizaciju prirodnih brojeva (na čemu se temelji RSA), za koje su najbolji poznati algoritmi subeksponencijalni. To znači da su ključevi potrebni za jednaku sigurnost osjetno kraći kod kriptografije eliptičkih krivulja.
U ovom radu bavimo se jednostavnijim dijelom eliptičkih krivulja, preciznije osnovama i osnovnim operacijama kod eliptičkih krivulja nad konačnim poljima. Rad je podijeljen na tri poglavlja gdje su prva dva priprema za treće.
Prvo poglavlje nas upoznaje s osnovnim algebarskim strukturama i poziva se na [1] i na [3]. Ovdje se definiraju osnovni pojmovi koji nas dovode do definicije polja, koja nam je nužna za nastavak rada.
Drugo poglavlje nas uvodi u eliptičke krivulje, te nas upoznaje s eliptičkim krivuljama i s osnovnim operacijma nad eliptičkim krivuljama. Ovo poglavlje se zove na [1] i [4].
Treće poglavlje nas upoznaje sa različitim koordinatama kod kojih se mijenja složenost osnovnih operacija nad eliptičkim krivuljama. Upoznajemo se s afinim, projektivnim, Jacobijevim i varijacijama na Jacobijeve te s miješanim koordinatama, te se složenosti osnovnih operacija uspoređuju u različitim koordinatama. Ovo poglavlje zove se na [1] , [2] te [4].

Poglavlje 1

Osnovne algebarske strukture

Počet ćemo od definiranja grupe, zatim ćemo isto napraviti s prstenovima te s poljima za kraj ovog poglavlja.

1.1 Grupe

Definicija 1.1.1. *Neprazan skup $G = (G, \cdot)$, gdje je $\cdot : G \times G \to G$ binarna operacija, zove se grupa ako vrijede slijedeća svojstva:*

$$1)\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \quad \forall x, y, z \in G \quad (asocijativnost);$$

$$2)\ (\exists e \in G) : e \cdot x = x \cdot e = x \quad \forall x \in G \quad (neutralni\ element);$$

$$3)\ (\forall x \in G)(\exists! x^{-1} \in G) : x \cdot x^{-1} = x^{-1} \cdot x = e \quad (inverzni\ element).$$

Napomena:
Ako vrijedi $x \cdot y = y \cdot x$, $\forall x, y \in G$, onda kažemo da je G komutativna ili Abelova grupa.

1.2 Prstenovi

Definicija 1.2.1. *Neprazan skup $R = (R, +, \cdot)$ zovemo prsten ako je za operacije zbrajanja $+ : R \to R$ i množenja $\cdot : R \times R \to R$ ispunjeno slijedeće:*

$$1)\ (R, +)\ je\ komutativna\ grupa,\ s\ neutralnim\ elementom\ 0 = 0_R;$$

$$2)\ (R, \cdot)\ je\ polugrupa,\ to\ jest\ množenje\ je\ asocijativno;$$

3) *Vrijedi distributivnost množenja prema zbrajanju, to jest* :

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \forall x, y, z \in R$$

$$(x + y) \cdot z = x \cdot z + y \cdot z \quad \forall x, y, z \in R.$$

Napomene:
Element $0 = 0_R$, neutralni element u grupi $(R, +)$, zvat ćemo nula prstena R.
Ako postoji jedinični element ili kraće jedinica, $1 = 1_R \in R$ takav da je $1 \cdot x = x \cdot 1 = x$, $\forall x \in R$, onda kažemo da je R prsten s jedinicom.
Prsten R je komutativan prsten ako je $x \cdot y = y \cdot x$, $\forall x, y \in R$; inače govorimo o nekomutativnom prstenu.

1.3 Polja

Definicija 1.3.1. *Prsten R je tijelo ili prsten s dijeljenjem, ako je svaki ne-nul element u R invertibilan, to jest ukoliko je* $R^x = R \setminus \{0\}$.
Komutativno tijelo zove se ***polje****.*

Definicija 1.3.2. *Ako su* $\mathbb{K}$, $\mathbb{L}$ *polja takva da je* $\mathbb{K} \subset \mathbb{L}$, *onda kažemo da je* $\mathbb{K}$ *potpolje od* $\mathbb{L}$ *ili da je* $\mathbb{L}$ *proširenje od* $\mathbb{K}$. *Oznaka je* $\mathbb{L}/\mathbb{K}$.

Definicija 1.3.3. *Polje je prosto polje ako ne sadrži niti jedno pravo potpolje.*

Teorem 1.3.4. *U svakom polju* $\mathbb{K}$ *sadžano je jedinstveno prosto potpolje* $\mathbb{K}_0$. *Nadalje imamo točno jednu od sljedeće dvije mogućnosti:*

$$1)\ \mathbb{K}_0 \cong \mathbb{Q} \text{ i tada } char\mathbb{K} = 0;$$

$$2)\ \mathbb{K}_0 \cong \mathbb{Z}/p\mathbb{Z} \text{ i tada } char\mathbb{K} = p, \text{ gdje je } p \text{ prim broj.}$$

Dokaz. Dokaz se nalazi u [3]. □

Algebarska proširenja polja

Ako imamo proširenje polja $\mathbb{L}/\mathbb{K}$, onda možemo gledati $\mathbb{L}$ kao vektorski prostor nad $\mathbb{K}$. Označimo $[\mathbb{L} : \mathbb{K}] := dim_{\mathbb{K}}\mathbb{L}$.

Definicija 1.3.5. *Kažemo da je* $\mathbb{L}/\mathbb{K}$ *konačno proširenje ako je* $[\mathbb{L} : \mathbb{K}] < \infty$.

Definicija 1.3.6. *Kažemo da je $\alpha \in \mathbb{L}$ algebarski nad $\mathbb{K}$, ako postoji polinom $0 \neq F \in \mathbb{K}[X]$ takav da je:*

$$F(\alpha) = 0, \text{ to jest } \alpha \text{ je nultočka od } F;$$

inače kažemo da je α transcedentan nad $\mathbb{K}$.

Definicija 1.3.7. *Kažemo da je proširenje $\mathbb{L}/\mathbb{K}$ algebarsko (nad $\mathbb{K}$), ako je svaki $\alpha \in \mathbb{L}$ algebarski, nad $\mathbb{K}$. Općenito, ako imamo proširenje $\mathbb{L}/\mathbb{K}$, onda je*

$$\mathbb{E} := \{\alpha \in \mathbb{L} \mid \alpha \text{ algebarski nad } \mathbb{K}\}$$

polje; takozvano algebarsko zatvorenje od $\mathbb{K}$ u $\mathbb{L}$.

Definicija 1.3.8. *Kažemo da je polje $\mathbb{K}$ algebarski zatvoreno, ako svaki nekonstantan polinom iz $\mathbb{L}[X]$ ima bar jednu nultočku u $\mathbb{K}$. (Lako se vidi da su onda sve nultočke, bilo kojeg nekonstantnog polinoma iz $\mathbb{K}$).*

Teorem 1.3.9. *Za svako polje $\mathbb{K}$ postoji algebarsko proširenje $\mathbb{L}/\mathbb{K}$ takvo da je $\mathbb{L}$ algebarski zatvoreno polje. Nadalje, ako su $\mathbb{L}_1$ i $\mathbb{L}_2$ dva algebarska proširenja od $\mathbb{K}$, i oba su algebarski zatvorena, onda postoji izomorfizam polja $\sigma : \mathbb{L}_1 \to \mathbb{L}_2$ nad $\mathbb{K}$.*

Polje $\mathbb{L}$ iz prethodnog teorema (koje je, do na izomorfizam, jedinstveno) zovemo algebarski zatvarač od $\mathbb{K}$, i označavamo sa $\overline{\mathbb{K}}$; to jest:
$\overline{\mathbb{K}}$:= algebarski zatvarač od $\mathbb{K}$.

Poglavlje 2

Eliptičke krivulje

2.1 Osnove eliptičkih krivulja

U ovom poglavlju se bavimo pozadinom eliptičkih krivulja i aritmetikom eliptičkih krivulja.

Definicija 2.1.1. *Neka je $\mathbb{K}$ polje. Karakteristika polja $\mathbb{K}$ je najmanji prirodni broj n takav da je $1 + 1 + 1 + \cdots + 1 = n \cdot 1 = 0$, gdje su 0 i 1 neutralni elementi za zbrajanje, odnosno množenje u $\mathbb{K}$. Ako je $n \cdot 1 \neq 0$ za svaki prirodan broj n, onda se kaže da je $\mathbb{K}$ polje karakteristike 0.*

Definicija 2.1.2. *Eliptička krivulja E nad poljem $\mathbb{K}$ označena s $E/\mathbb{K}$ je dana s Weierstrassovom jednadžbom:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

gdje su koeficijenti $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$ te u svakoj točki (x_1, y_1) s koordinatama u $\overline{\mathbb{K}}$ koja zadovoljava gornju jednadžbu te parcijalne derivacije $2y_1+a_1x_1+a_3$ i $3x_1^2+2a_2x_1+a_4-a_1y_1$ nisu istovremeno jednake nuli.

Zadnji uvjet osigurava da je krivulja glatka. Točka na krivulji je singularna ako su obje parcijalne derivacije u toj točki jednake nuli.
Označimo s:

$$b_2 = a_1^2 + 4a_2 \qquad b_4 = a_1a_3 + 2a_4$$

$$b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2 a_6 - a_1 a_3 a_4 + 4a_2 a_6 + a_2 a_3^2 - a_4^2$$

Ove oznake nam pojednostavljuju slijedeću definiciju:

Definicija 2.1.3. *Neka je E krivulja definirana nad $\mathbb{K}$, te $b_2, b_4, b_6 i b_8$ definirani kao gore. Diskriminanta krivulje E, označena s Δ zadovoljava:*

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6.$$

Krivulja E je nesingularna pa tako i eliptička ako i samo ako Δ je različita od nule. Ako je to slučaj uvodimo j-invarijantu od E:

$$j(E) = (b_2^2 - 24b_4)^3/\Delta.$$

2.2 Zbrajanje točaka na eliptičkim krivuljama

Neka je E eliptička krivulja kako smo ju definirali. Skup točaka krivulje E možemo prikazati kao grupu s operacijom $\oplus$ koju ćemo zvati zbrajanje.
Da bi smo zbrojili dvije točke $P = (x_1, y_1)$ i $Q = (x_2, y_2)$ povučemo pravac koji ih povezuje. Postoji treća točka presjeka pravca PQ i krivulje E. Nazovimo tu točku R'. Zatim zrcalimo točku R' preko x-osi, da bi smo dobili točku R. Točka R nam je suma točaka P i Q, a to zapisujemo:

$$R = P \oplus Q.$$

Dalje, moramo definirati zbroj dvije točke s istom x-koordinatom, jer za njih se operacija zbrajanja u grupi ne može provesti kako smo pokazali. Za neki x_1 postoje najviše dvije takve točke, (x_1, y_1) i $(x_1, -y_1)$. Još moramo naći i neutralni element.
Oba problema se rješavaju uvođenjem dodatne točke P_∞ koju zovemo točka u beskonačnosti. P_∞ možemo vizualizirati kao točku na kraju y-osi tako da svaki pravac $x = c$, za neku konstantu c, paralelan sa y-osi prolazi kroz P_∞. Dakle, pravac koji povezuje (x_1, y_1) i $(x_1, -y_1)$ prolazi kroz P_∞.

$$(x_1, y_1) \oplus (x_1, -y_1) = P_\infty.$$

Dosad napisano izgleda kao da funkcionira samo za polje $\mathbb{R}$, no sada ćemo izvesti formule

koje vrijede za proizvoljno polje $\mathbb{K}$.
Uzmimo $P \neq Q$ sa $x_1 \neq x_2$ te izračunajmo koordinate točke $R = P \oplus Q = (x_3, y_3)$. Pravac koji prolazi kroz P i Q ima koeficijent smjera:

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

te znamo da prolazi kroz točku P, iz čega lako izvlačimo jednadžbu pravca:

$$y = \lambda x + \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2}.$$

Sad konstantni dio označimo sa μ te primjetimo $\mu = y_1 - \lambda x_1$. Točke gdje pravac siječe krivulju dobivamo uvrštavanjem:

$$(\lambda x + \mu)^2 + (a_1 x + a_3)(\lambda x + \mu) = x^3 + a_2 x^2 + a_4 x + a_6,$$

što nas vodi do jednadžbe $r(x) = 0$ gdje

$$r(x) = x^3 + (a_2 - \lambda^2 - a_1\lambda)x^2 + (a_4 - 2\lambda\mu - a_3\lambda - a_1\mu)x + a_6 - \mu^2 - a_3\mu.$$

Već znamo dva korijena ovog polinoma, specifično x-koordinate od P i Q. Imamo

$$r(x) = (x - x_1)(x - x_2)(x - x_3),$$

što raspišemo kao

$$r(x) = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3,$$

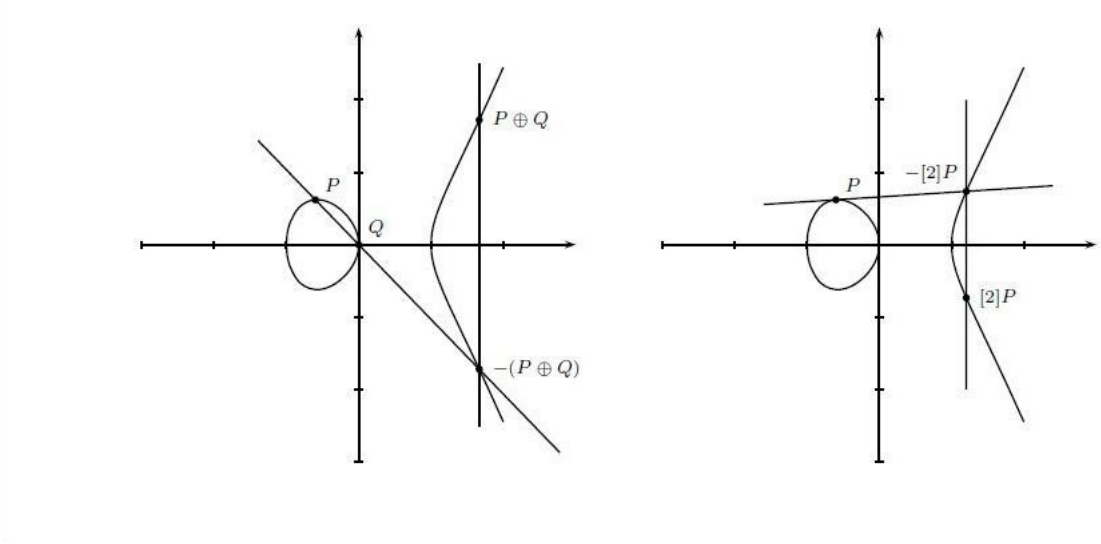
sada izjednačimo članove uz x^2 :

$$\lambda^2 + a_1\lambda - a_2 = x_1 + x_2 + x_3.$$

Kako su x_1 i x_2 definirani nad $\mathbb{K}$, tako je i x_3 te $\tilde{y_3} = \lambda x_3 + \mu$. Točka koju tražimo mora imati istu x-koordinatu te zadovoljavati jednadžbu krivulje. Primjetimo da ako je $P = (x_1, y_1)$ na krivulji, tada je i $(x_1, -y_1 - a_1x_1 - a_3)$ što odgovara točki - P. Analogno nalazimo da je $y_3 = -\lambda x_3 - \mu - a_1x_3 - a_3$.
Postavlja se pitanje što se događa kad želimo zbrojiti točku samu sa sobom. Točku $P = (x_1, y_1)$ dupliciramo (zbrajamo samu sa sobom) na isti način kao što zbrajamo dvije točke,

samo što više ne možemo gledati sekantu za koeficijent pravca, već moramo gledati tangentu, a koeficijent smjera tangente dobivamo deriviranjem. Tako imamo $P \oplus Q = (x_3, y_3)$ i

$$-P = (x_1, -y_1 - a_1x_1 - a_3),$$
$$P \oplus Q = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3), \ gdje$$
$$\lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{ako } P \neq \pm Q \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{ako } P = Q. \end{cases}$$



Slika 2.1: Geometrijski prikaz zbrajanja i dupliciranja

Ovako definirano zbrajanje na E jest grupa. Sa slikom kao vizualnim pomagalom, komutativnost je očita, računski smo pokazali da je točka u beskonačnosti neutral, te da je inverz (x_1, y_1) dan s $(x_1, -y_1 - a_1x_1 - a_3)$. Jedino je asocijativnost složenija za pokazati, nećemo to pokazivati u ovom radu, ali ima zgodna animacija na [5] te dokaz u [6] .

2.3 Množenje skalarom

Potenciranje je vrlo važna operacija u algoritamskoj teoriji brojeva, intenzivno se koristi u testiranju prostosti i algoritmima za faktoriranje. Efikasne metode su bile proučavane stoljećima. Potenciranje često troši najviše vremena u kriptosustavima koji se temelje na problemu diskretnog logaritma te određuje složenost kriptografskih protokola kao razmjena ključeva, autentifikacija i potpisivanje.

U kontekstu eliptičkih krivulja, ekvivalent potenciranja x^n je množenje skalarom $[n]P$. Prilagodbe su trivijalne, zamjenjuje se množenje sa zbrajanjem i kvadriranje s dupliciranjem. Uzmimo $n \in \mathbb{N} \setminus \{0\}$ i označimo skalarnu multiplikaciju sa n na E sa $[n]$, ili, da izbjegnemo zabune, sa $[n]_E$. Precizno zapisano:

$$[n] : E \to E$$

$$P \mapsto [n]P = \underbrace{P \oplus P \oplus \ldots \oplus P}_{\text{n puta}}$$

Definicija se prirodno proširuje na sve $n \in \mathbb{Z}$, postavljajući $[0]P = P_\infty$ i $[n]P = [-n](-P)$ za $n < 0$.

Postoji nekoliko algoritama za potenciranje ili množenje skalarom. Neki od njih su binarna metoda s lijeva na desno; binarna metoda s desna na lijevo; Montgomeryjeve ljestve; 2^k algoritam s lijeva na desno; algoritam prozora, svaki ima neke prednosti i mane, no prikazati ću samo jedan. Odabrao sam algoritam kliznog prozora.

Skalarna multiplikacija na eliptičkim krivuljama koristeći algoritam kliznog prozora

---

Ulaz: Točka P na eliptičkoj krivulji E, nenegativni prirodni broj n, zapisan binarno kao $n = (n_{r-1} \ldots n_0)_2$, parametar $k \geq 1$ i unaprijed izračunate točke $[3]P, [5]P, \ldots, [(2^k - 1)]P$.
Izlaz: Točka $[n]P$

1. $Q = P_\infty$ i = r − 1
2. while $(i \geq l - 1)$ do
3. if $(n_i == 0)$ then $Q = [2]Q$ and $i = i - 1$
4. else {
5. $s = max(i - k + 1, 0)$
6. while $(n_s == 0)$ do $s = s + 1$
7. for $(h = 1; h \leq i - s + 1; h++)$ Q=[2]Q
8. $u = (n_i \ldots n_s)_2$ // u je uvijek neparan

9. $Q = Q \oplus [u]P$
10. $i = s - 1\}$
11. return Q

Kod algoritma kliznog prostora "razrežemo" binarni oblik broja n u dijelove koristeći prozor duljine k te obrađujemo dijelove jedan po jedan. Također algoritam kliznog prozora nam omogućava da ignoriramo nizove uzastopnih nula, što možemo još bolje iskoristiti nakon uvođenja slijedećih pojmova.

Rekodiranje znamenki s predznakom: Ako imamo sustav gdje je računanje inverza (dijeljenje za naše svrhe) brzo, može biti vrlo efikasno množiti sa x ili x^{-1}. To nam može uštedjeti dodatna množenja, ali dolazi uz cijenu da dozvoljavamo negativne koeficijente. Ekstreman primjer takve situacije je računanje 2^{2^k-1}. Uobičajenom metodom, treba nam $k-1$ kvadriranje i $k-1$ množenje. Ako dozvolimo x^{-1}, treba nam k kvadriranja i jedno množenje sa x^{-1}. To nas vodi do slijedećeg koncepta:

Definicija 2.3.1. *Prikaz znamenki s predznakom cijelog broja n u bazi b je dan s*

$$n = \sum_{i=1}^{l-1} n_i b^i \qquad gdje\ |n_i| < b.$$

Prikaz znamenki s predznakom označavamo sa $(n_l - 1 \dots n_0)_s$ i obično se dobije nekom metodom rekodiranja. Za prikaz znamenki s predznakom kažemo da je u ne-susjednoj formi ("non-adjacent form"; dalje u tekstu koristimo kraticu NAF), ako $n_i n_{i+1} = 0 \ \forall i \geq 0$ i označavamo ga s $(n_{l-1} \dots n_0)_{NAF}$.

Na primjer, prikaz u obliku binarnog zapisa s predznakom odgovara specifičnom izboru $b = 2$ i $n_i \in \{-1, 0, 1\}$ te -1 označimo sa $\overline{1}$. Uzmimo $n = 478$. Tada je $478 = (111011110)_2 = (100\overline{1}100\overline{1}0)_s$. No prikaz u obliku znamenki s predznakom nije jedinstven. NAF jest te $478 = (1000\overline{1}00\overline{1}0)_{NAF}$. U prosjeku broj nenul znamenki u NAF izrazu duljine l je jednak $l/3$.

Algoritam za reprezentaciju NAF

Ulaz: Prirodni broj $n = (n_l n_{l-1} \dots n_0)_2$ s tim da $n_l = n_{l-1} = 0$.
Izlaz: NAF zapis broja n

1. $c_0 = 0$
2. for $(i = 0; i <= l - 1; i++)$
3. $\quad c_{i+1} = \lfloor (c_i + n_i + n_{i+1})/2 \rfloor$
4. $\quad n'_i = c_i + n_i - 2c_{i+1}$
5. return $(n'_{l-1} \ldots n'_0)_{NAF}$

Definicija 2.3.2. *Neka je w parametar veći od 1. Tada svaki prirodni broj n ima jedinstveni prikaz u obliku znamenaka s predznakom*

$$n = \sum_{i=0}^{l-1} n_i 2^i,$$

gdje svaki n_i je nula ili neparan; $|n_i| < 2^{w-1}$; među bilo koliko w koeficijenata zaredom najviše jedan je različit od nule.

Proširenje ove forme zovemo ne-susjedna forma širine w, kratica NAF_w i zapisujemo $(n_{l-1} \ldots n_0)_{NAF_w}$.

Algoritam za reprezentaciju NAF_w

Ulaz: Prirodni broj $n = (n_l n_{l-1} \ldots n_0)_2$ s tim da $n_l = n_{l-1} = 0$.
Izlaz: NAF zapis broja n

1. $i = 0$
2. while $n > 0$ do
3. $\quad$ if n is odd then
4. $\quad\quad n_i = n \bmod 2^w$
5. $\quad\quad n = n - n_i$
6. $\quad$ else $n_i = 0$
7. $\quad n = n/2$ and $i = i + 1$
8. return $(n_{l-1} \ldots n_0)_{NAF_w}$

Sada možemo iskoristiti algoritam kliznog prozora u kombinaciji sa zapisom brojeva u NAF_w obliku. Time dobivamo mogućnost da ignoriramo nizove uzastopnih nula, koje će

se pojavljivati zbog NAF_w zapisa.
Prosječna duljina niza nuli između prozora je

$$v(k) = \frac{4}{3} - \frac{(-1)^k}{3 \cdot 2^{k-2}},$$

a očekivano trajanje algoritma je

$$\left[1D + \left(\frac{2^k - (-1)^k}{3} - 1\right)Z\right] + \frac{m}{k + v(k)}Z + mD,$$

gdje je k širina prozora, $m = \lceil \log_2 q \rceil$ gdje je q red polja nad kojim se eliptička krivulja E nalazi, D je dupliciranje, a Z zbrajanje.
Razlog za odabir algoritma kliznog prozora je lijepo kombiniranje sa zapisom u NAF_w, mogućnost iskorištavanja unaprijed izračunatih vrijednosti, relativno bolja efikasnost u usporedbi sa većinom ostalih navedenih algoritama, te nema slabost Montgomeryevog algoritma [7].

Poglavlje 3

Aritmetika eliptičkih krivulja nad konačnim poljima

U ovom poglavlju promatramo krivulje definirane nad konačnim prostim poljima $\mathbb{F}_p$. Kako se ta polja primjenjuju u kriptografiji, možemo pretpostaviti da je p velik, barem $p > 3$. Napominjemo da sve tvrdnje u ovom poglavlju vrijede za eliptičke krivulje definirane nad proizvoljnim konačnim poljem $\mathbb{F}_q$ ako $char(\mathbb{F}_q) > 3$ i za supersingularne krivulje nad poljem karakteristike 3.
Napomena: U ovom diplomskom radu se ne bavimo supersingularnim eliptičkim krivuljama.
Promatrat ćemo brzine zbrajanja i dupliciranja u različitim koordinatnim sustavima. Složenost mjerimo brojem operacija u polju potrebnih da bi se ostvarila tražena operacija (zbrajanje ili dupliranje). Operacije u polju su elementarno množenje, kvadriranje i inverz za množenje (dijeljenje).
Da si olakšamo, uvodimo kratku Weierstrassovu formu, koju izvodimo iz Weierstrassove forme na slijedeći način:
Uzmemo Weierstrassovu formu:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Uvodimo supstituciju $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ kojom eliminiramo sve članove koji sadrže y, osim y^2. Supstituciju smijemo koristiti jer karakteristika polja nije dva, pa smijemo dijeliti s dva. Dobivamo:

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

gdje

$$b_2 = a_1^2 + 4a_2,$$

$$b_4 = a_1a_3 + 2a_4,$$

$$b_6 = a_3^2 + 4a_6.$$

Jer je karakteristika različita i od tri, možemo uvesti slijedeće supstitucije: $x \mapsto \frac{x-3b_2}{36}$ i $y \mapsto \frac{y}{108}$, čime dobivamo jednadžbu u kratkoj Weierstrassovoj formi:

$$y^2 = x^3 - 27c_4x - 54c_6,$$

gdje

$$c_4 = b_2^2 - 24b_3,$$

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Kratka Weierstrassova forma se češće zapisuje kao:

$$E : y^2 = x^3 + a_4 + a_6,$$

gdje to očito nisu isti a_4 i a_6 kao u punoj Weierstrassovoj formi.

3.1 Afine koordinate

Pretpostavimo da je eliptička krivulja E zadana s kratkom Weierstrassovom formom:

$$y^2 = x^3 + a_4x + a_6,$$

Kratka Weierstrassova forma nam olakšava račun jer točka nasuprot točke (x_1, y_1) je točka $(x_1, -y_1)$.

Zbrajanje: Neka su točke $P = (x_1, y_1)$, $Q = (x_2, y_2)$ takve da $P \neq \pm Q$ i $P \oplus Q = (x_3, y_3)$. Sada je zbrajanje dano sa:

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1, \quad \lambda = \frac{y_1 - y_2}{x_1 - x_2}.$$

Složenost zbrajanja je jedno dijeljenje, dva množenja i jedno kvadriranje.

Dupliciranje: Neka je $[2]P = (x_3, y_3)$. Tada

$$x_3 = \lambda^2 - 2x_1, \quad y_3 = \lambda(x_1 - x_3) - y_1, \quad \lambda = \frac{3x_1^2 + a_4}{2y_1}.$$

Složenost dupliciranja je jedno dijeljenje, dva množenja i dva kvadriranja.

Dupliciranje praćeno zbrajanjem: Smišljeno da ubrza računanje u nekim situacijama, ideja je da se koristi $[2]P \oplus Q$ umjesto $(P \oplus Q) \oplus P$. Za $P \neq \pm Q$ i $[2]P \neq Q$ imamo slijedeće formule:

$$A = (x_2 - x_1)^2, \qquad B = (y_2 - y_1)^2, \qquad C = A(2x_1 + x_2) - B,$$
$$D = C(x_2 - x_1), \qquad E = D^{-1}, \qquad \lambda = CE(y_2 - y_1),$$
$$\lambda_2 = 2y_1A(x_2 - x_1)E - \lambda, \quad x_4 = (\lambda_2 - \lambda)(\lambda + \lambda_2) + x_2, \quad y_4 = (x_1 - x_4)\lambda_2 - y_1.$$

Složenost je jedno dijeljenje, devet množenja i dva kvadriranja. Primjetimo da korištenjem ovih formula ne moramo računati x_3 i y_3 te da su efikasnije kad god je dijeljenje u polju skuplje od 6 množenja.

3.2 Projektivne koordinate

Zašto projektivne koordinate?
Kod zbrajanja i dupliciranja u afinim koordinatama, moramo dijeliti. No dijeljenje je množenje s inverzom. Dakle moramo izračunati inverz. Postoji nekoliko algoritama za računanje inverza, najpoznatiji je prošireni Euklidov algoritam, postoji još i plus-minus algoritam, Montgomeryev algoritam za inverz i tako dalje, no svi oni imaju nešto zajedničko. Svaki od navedenih algoritama je skup u odnosu na množenje i kvadriranje. Po procjenama [1] (u prosjeku) kvadriranje traje oko 0.8 množenja, a dijeljenje između 9 i 40 množenja. Projektivne koordinate uvodimo da bi izbjegli dijeljenje, te tako ubrzali operacije zbrajanja i dupliciranja. Za primjer navodimo prošireni Euklidov algoritam za prirodne brojeve i modificirani prošireni Euklidov algoritam za inverz u $\mathbb{F}_p$:

Prošireni Euklidov algoritam za prirodne brojeve

Ulaz: Prirodni brojevi a i b takvi da $a \leq b$.
Izlaz: $d = nzd(a,b)$ i prirodni brojevi x,y takvi da zadovoljavaju $ax + by = d$

1. $u = a$, $v = b$
2. $x_1 = 1$, $y_1 = 0$, $x_2 = 0$, $y_2 = 1$
3. While $u \neq 0$ do
4. $\quad q = \lfloor v/u \rfloor$, $r = v - qu$, $x = x_2 - qx_1$ $y = y_2 - qy_1$.
5. $\quad v = u$, $u = r$, $x_2 = x_1$, $x_1 = x$ $y_2 = y_1$, $y_1 = y$.
6. $d = v$, $x = x_2$, $y = y_2$
7. return (d, x, y)

Inverz u $\mathbb{F}_p$ koristeći prošireni Euklidov algoritam za prirodne brojeve

Ulaz: p prost broj i $a \in [1, p-1]$
Izlaz: $a^{-1} \bmod p$

1. $u = a$, $v = p$
2. $x_1 = 1$, $x_2 = 0$
3. While $u \neq 1$ do
4. $\quad q = \lfloor v/u \rfloor$, $r = v - qu$, $x = x_2 - qx_1$.
5. $\quad v = u$, $u = r$, $x_2 = x_1$, $x_1 = x$.
6. return $x_1 \bmod p$

Nakon što smo objasnili zašto koristimo projektivne koordinate, prikaz eliptičke krivulje E bio bi sljedeći:

$$Y^2Z = X^3 + a_4Z^2 + a_6Z^3.$$

Točka $(X_1 : Y_1 : Z_1)$ na E odgovara afinoj točki $(X_1/Z_1, Y_1/Z_1)$ kada $Z_1 \neq 0$, a točki u beskonačnosti $P_\infty = (0 : 1 : 0)$ inače. Točka nasuprot $(X_1 : Y_1 : Z_1)$ je $(X_1 : -Y_1 : Z_1)$.

Zbrajanje: Neka su $P = (X_1 : Y_1 : Z_1)$ i $Q = (X_2 : Y_2 : Z_2)$ takve točke da $P \neq \pm Q$ i $P \oplus Q = (X_3 : Y_3 : Z_3)$. Radi lakše notacije, stavimo:

$$A = Y_2Z_1 - Y_1Z_2, \quad B = X_2Z_1 - X_1Z_2, \quad C = A^2Z_1Z_2 - B^3 - 2B^2X_1Z_2$$

pa imamo:

$$X_3 = BC, \quad Y_3 = A(B^2X_1Z_2 - C) - B^3Y_1Z_2, \quad Z_3 = B^3Z_1Z_2.$$

Složenost zbrajanja je dvanaest množenja i dva kvadriranja. Dijeljenje nam ne treba. Ako je jedna od ulaznih točaka dana sa $(X_2 : Y_2 : 1)$ to jest direktno transformirana iz afinih koordinata, tada je složenost devet množenja i dva kvadriranja.

Dupliciranje: Neka je $[2]P = (X_3, Y_3, Z_3)$ te si olakšamo notaciju na sličan način kao kod zbrajanja:

$$A = a_4 Z_1^2 + 3X_1^2, \quad B = Y_1 Z_1, \quad C = X_1 Y_1 B, \quad D = A^2 - 8C,$$

tada imamo

$$X_3 = 2BD, \qquad Y_3 = A(4C - D) - 8Y_1^2 B^2, \qquad Z_3 = 8B^3.$$

Složenost dupliciranja je sedam množenja i pet kvadriranja.

3.3 Jacobijeve i Chundovsky-Jacobijeve koordinate $\mathcal{J}$ i $\mathcal{J}^c$

U Jacobijevim koordinatama krivulja E je dana sa

$$Y^2 = X^3 + a_4 XZ^4 + a_6 Z^6.$$

Točka $(X_1 : Y_1 : Z_1)$ na E odgovara afinoj točki $(X_1/Z_1^2, Y_1/Z_1^3)$ kada $Z_1 \neq 0$, a točki u beskonačnosti $P_\infty = (1 : 1 : 0)$ inače. Točka nasuprot $(X_1 : Y_1 : Z_1)$ je $(X_1 : -Y_1 : Z_1)$.

Zbrajanje: Neka su $P = (X_1 : Y_1 : Z_1)$ i $Q = (X_2 : Y_2 : Z_2)$ takve točke da $P \neq \pm Q$ i $P \oplus Q = (X_3 : Y_3 : Z_3)$. Radi lakše notacije, stavimo:

$$A = X_1 Z_2^2, \quad B = X_2 Z_1^2, \quad C = Y_1 Z_2^3, \quad D = Y_2 Z_1^3, \quad E = B - A, \quad F = D - C$$

pa imamo:

$$X_3 = -E^3 - 2AE^2 + F^2, \quad Y_3 = -CE^3 + F(AE^2 - X_3), \quad Z_3 = Z_1 Z_2 E.$$

Složenost zbrajanja je dvanaest množenja i četiri kvadriranja. Ako je jedna od točaka zadana u obliku $(X_1 : Y_1 : 1)$ složenost zbrajanja je smanjena na osam množenja i tri kvadriranja.

Dupliciranje: Neka $[2]P = (X_3 : Y_3 : Z_3)$. Radi lakše notacije, stavimo:

$$A = 4X_1 Y_1^2, \qquad B = 3X_1^2 + a_4 Z_1^4$$

pa imamo:

$$X_3 = -2A + B^2, \quad Y_3 = -8Y_1^4 + B(A - X_3), \quad Z_3 = 2Y_1 Z_1.$$

Složenost dupliciranja je četiri množenja i šest kvadriranja.

U Jacobijevim koordinatama dupliranja su brža, a zbrajanja sporija nego u projektivnim koordinatama. Da poboljšamo zbrajanje, točka P je predstavljena kao petorka $(X_1, Y_1, Z_1, Z_1^2, Z_1^3)$. Te koordinate zovemo Chundovsky-Jacobijeve koordinate. Zbrajanja i dupliranja su dana sa istim formulama kao za $\mathcal{J}$, ali složenosti su jedanaest množenja i tri kvadriranja za zbrajanje te pet množenja i šest kvadriranja za dupliciranje.

3.4 Modificirane Jacobijeve koordinate $\mathcal{J}^m$

Modificirane Jacobijeve koordinate su utemeljene na Jacobijevim, ali je reprezentacija točke P četvorka $(X_1, Y_1, Z_1, a_4 Z_1^4)$.

Zbrajanje: Neka su $P = (X_1 : Y_1 : Z_1)$ i $Q = (X_2 : Y_2 : Z_2)$ takve točke da $P \neq \pm Q$ i $P \oplus Q = (X_3 : Y_3 : Z_3)$. Radi lakše notacije, stavimo:

$$A = X_1 Z_2^2, \quad B = X_2 Z_1^2, \quad C = Y_1 Z_2^3, \quad D = Y_2 Z_1^3, \quad E = B - A, \quad F = D - C$$

pa imamo:

$$X_3 = -E^3 - 2AE^2 + F^2, \quad Y_3 = -CE^3 + F(AE^2 - X_3), \quad Z_3 = Z_1 Z_2 E \quad a_4 Z_3^4 = a_4 Z_3^4.$$

Složenost zbrajanja je trinaest množenja i šest kvadriranja. No, ako uzmemo jednu točku u afinim koordinatama (X_2, Y_2), složenost se mijenja u devet množenja i pet kvadriranja.

Dupliciranje: Neka $[2]P = (X_3 : Y_3 : Z_3)$. Radi lakše notacije, stavimo:

$$A = 4X_1 Y_1^2, \qquad B = 3X_1^2 + a_4 Z_1^4 \qquad C = 8Y_1^4$$

pa imamo:

$$X_3 = -2A + B^2, \quad Y_3 = B(A - X_3) - C, \quad Z_3 = 2Y_1 Z_1, \quad a_4 Z_3^4 = 2C(a_4 Z_1^4).$$

Složenost dupliciranja je četiri množenja i četiri kvadriranja.

Kako dijeljenje traje u prosjeku između devet i 40 množenja, a kvadriranje oko 0.8 množenja, ovaj sustav nudi najbrži postupak za dupliranje.

3.5 Miješane koordinate

Unatoč ubrzanju koje smo ostvarili s različitim koordinatnim sustavima, želimo ostvariti još brže izvođenje zbrajanja i dupliciranja. Način na koji ćemo to postići je korištenjem različitih sustava koordinata koje smo definirali ranije. To znači da možemo zbrajati i duplicirati točke izražene u dva različita sustava i dati rezultat u trećem. Na primjer $\mathcal{J}+\mathcal{J}^c = \mathcal{J}^m$ znači da možemo zbrojiti točke u Jacobijevim i Chudnovsky Jacobijevim koordinatama, te izraziti rezultat u modificiranim Jacobijevim koordinatama. Cilj je izabrati najefikasnije kombinacije za svaku operaciju koju izvodimo.

Pretpostavimo da želimo izračunati $[n]P$. Koristiti ćemo NAF_w prikaz od n. Dakle moramo unaprijed izračunati $[i]P$ za svaki neparan i takav da $1 < i < 2^{w-1}$. Za te proračune korisno je odabrati ili afine koordinate, ako se neka dijeljenja mogu izvesti u toj fazi ili Chundovsky-Jacobijeve koordinate ($\mathcal{J}^c$) jer ta dva sustava daju najefikasnije miješane formule za zbrajanje. Ako smo odabrali afine koordinate, trebamo koristiti Montgomeryjev trik istovremenih inverzija u $\mathbb{F}_p$.To vodi do

$$(w-1)D + (5x2^{w-2} + 2w - 12)M + (2^{w-2} + 2w - 5)K$$

broja operacija za računanje unaprijed, gdje D označava dijeljenje, M množenje, a K kvadriranje.

Montgomeryjev trik istovremenih inverzija u $\mathbb{F}_p$

Ulaz: prirodni broj p i k prirodnih brojeva $a_1,\ldots,a_k$ koji su različiti od 0 modulo p
Izlaz: inverzi $b_1,\ldots,b_j$ od $a_1,\ldots,a_j$ modulo p

1. $c_1 = a_1$
2. for $(i = 2; i \leq k; i++)$ do $c_i = c_{i-1}a_i \mod p$
3. $u = c_k^{-1} \mod p$
4. for $(i = k; i \geq 2; i--)$ do
5. $\quad a_i^{-1} = uc_{i-1} \mod p$
6. $\quad u = ua_i \mod p$
7. $a^{-1} = u$
8. return $(a_1^{-1},\ldots,a_k^{-1})$

Dijeljenje u polju je skupo u usporedbi s množenjem. Ako nam trebaju inverzi za nekoliko elemenata, korištenjem ovog algoritma dobivamo inverze za tražene elemente pod "cijenu"

jednog inverza i tri množenja po elementu. Za k elemenata dakle, za "cijenu" jednog inverza i $3k$ množenja dobivamo k inverza.

U slijedećoj tablici uz već navedene kratice D, M i K; koristimo i $\mathcal{A}$ kao oznaku da koristimo afine koordinate; $\mathcal{P}$ za projektivne; $\mathcal{J}$ za Jacobijeve; $\mathcal{J}^c$ za Chundovsky-Jacobijeve; te $\mathcal{J}^m$ za modificirane Jacobijeve koordinate.

Tablica broja operacija potrebnih za zbrajanje i dupliranje u različitim koordinatama

Dupliranje		Zbrajanje	
Operacija	Cijena	Operacija	Cijena
$2\mathcal{P}$	$7M + 5K$	$\mathcal{J}^m + \mathcal{J}^m$	$13M + 6K$
$2\mathcal{J}^c$	$5M + 6K$	$\mathcal{J}^m + \mathcal{J}^c = \mathcal{J}^m$	$12M + 5K$
$2\mathcal{J}$	$4M + 6K$	$\mathcal{J} + \mathcal{J}^c = \mathcal{J}^m$	$12M + 5K$
$2\mathcal{J}^m = \mathcal{J}^c$	$4M + 5K$	$\mathcal{J} + \mathcal{J}$	$12M + 4K$
$2\mathcal{J}^m$	$4M + 4K$	$\mathcal{P} + \mathcal{P}$	$12M + 2K$
$2\mathcal{A} = \mathcal{J}^c$	$3M + 5K$	$\mathcal{J}^c + \mathcal{J}^c = \mathcal{J}^m$	$11M + 4K$
$2\mathcal{J}^m$	$3M + 4K$	$\mathcal{J}^c + \mathcal{J}^c$	$11M + 3K$
$2\mathcal{A} = \mathcal{J}^m$	$3M + 4K$	$\mathcal{J}^c + \mathcal{J} = \mathcal{J}$	$11M + 3K$
$2\mathcal{A} = \mathcal{J}$	$2M + 4K$	$\mathcal{J}^c + \mathcal{J}^c = \mathcal{J}$	$10M + 2K$
-	-	$\mathcal{J} + \mathcal{A} = \mathcal{J}^m$	$9M + 5K$
-	-	$\mathcal{J}^m + \mathcal{A} = \mathcal{J}^m$	$9M + 5K$
-	-	$\mathcal{J}^c + \mathcal{A} = \mathcal{J}^m$	$8M + 4K$
-	-	$\mathcal{J}^c + \mathcal{A} = \mathcal{J}^c$	$8M + 3K$
-	-	$\mathcal{J} + \mathcal{A} = \mathcal{J}$	$8M + 3K$
-	-	$\mathcal{J}^m + \mathcal{A} = \mathcal{J}$	$8M + 3K$
-	-	$\mathcal{A} + \mathcal{A} = \mathcal{J}^m$	$5M + 4K$
-	-	$\mathcal{A} + \mathcal{A} = \mathcal{J}^c$	$5M + 3K$
$2\mathcal{A}$	$D + 2M + 4K$	$\mathcal{A} + \mathcal{A}$	$D + 2M + K$

Množenje skalarom Množenje skalarom $[n]P$ sastoji se od niza dupliciranja i zbrajanja. Ako se koristi algoritam kliznog prozora modificiran s obzirom na predznak, često se pojavljuju nizovi dupliciranja sa svega par zbrajanja između. Dakle isplativo je razlikovati dupliciranje nakon kojeg slijedi dupliciranje i zadnje dupliciranje u nizu iza kojeg slijedi zbrajanje te odabrati različite koordinatne sustave za njih. Eksplicitno, za svaki nenul koeficijent u razvoju od n posredna varijabla Q je zamijenjena u svakom koraku sa

$$[2^s]Q \pm [u]P,$$

gdje $[u]P$ je u skupu unaprijed izračunatih vrijednosti. Dakle, zapravo izvodimo $(s-1)$ dupliranje tipa $2\mathcal{J}^m = \mathcal{J}^m$, dupliranje tipa $2\mathcal{J}^m = \mathcal{J}$ i zbrajanje $\mathcal{J} + \mathcal{A} = \mathcal{J}^m$ ili $\mathcal{J} + \mathcal{J}^c = \mathcal{J}^m$ ovisno o koordinatama unaprijed izračunatih vrijednosti.
Neka klizni prozor dio algoritma radi

$$n = 2^{n_0}(2^{n_1}(\dots 2^{n_{v-1}}(2^{n_v}W[v] + W[v-1])\dots) + W[0]),$$

gdje je $W[i]$ neparni cijeli broj za kojeg vrijedi $-2^{w-1}+1 \le W[i] \le 2^{w-1}-1$ za svaki $i, W[v] > 0, n_0 \ge 0$ i $n_i \ge w+1$ za $i \ge 1$. U glavnoj petlji izvodimo $u = \sum_{i=0}^{v} n_i$ dupliciranja i v zbrajanja. Postavimo $l_1 = l - (w-1)/2$ i $H = 1/2 - 1/(w+1)$. U prosjeku koristimo $(l_1 + H)$ dupliciranja i $(l_1 - H)/(w+1)$ zbrajanja. Tada trebamo približno

$$\left(l_1 + H + \frac{l_1 - H}{w+1}\right)D + \left(2(l_1+H) + \frac{2}{w+1}(l_1 - H)\right)M + \left(2(l_1+H) + \frac{2}{w+1}(l_1 - H)\right)K$$

da izračunamo $[n]P$ ne računajući cijenu unaprijed izračunatih vrijednosti ako su samo afine koordinate korištene,

$$\left(4(l_1+H) + \frac{8}{w+1}(l_1 - H)\right)M + \left(4(l_1+H) + \frac{5}{w+1}(l_1 - H)\right)K,$$

ako su unaprijed izračunate točke u $\mathcal{A}$ i račun je izvršen bez dijeljenja koristeći $\mathcal{J}$ i $\mathcal{J}^m$ za posredne točke i

$$\left(4(l_1+H) + \frac{11}{w+1}(l_1 - H)\right)M + \left(4(l_1+H) + \frac{5}{w+1}(l_1 - H)\right)K,$$

ako su unaprijed izračunate točke u $\mathcal{J}^c$. Ovisno o omjeru D/M, $\mathcal{A}$ ili $\mathcal{J}^c$ bi trebali biti odabrani. Na primjer za 192-bitni ključ biramo $\mathcal{A}$ ako $D < 33.9M$, a $\mathcal{J}^c$ inače.

Bibliografija

[1] H. Cohen, G. Frey,
”Handbook of Elliptic and Hyperelliptic Curve Cryprography”,
Chapman & Hall/CRC,
2006.

[2] D. Hankerson, A. Menezes, S. Vanstone,
”Guide to Elliptic Curve Cryptography”,
Springer,
2004.

[3] B. Širola, ”Algebarske strukture”, 2010.
http://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf , (2014.)

[4] A. Dujella, ”Eliptičke krivulje u kriptografiji”, 2013.
http://web.math.pmf.unizg.hr/ duje/elkript/elkripto2.pdf , (2014.)

[5] ”Elliptic curve”, 2014.
http://en.wikipedia.org/wiki/Elliptic_curve , (2014.)

[6] J. Silverman, J. Tate,
”Rational Points on Elliptic Curves”,
Springer,
1992.

[7] Y. Yarom, N. Benger,
”Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack”, 2014
https://eprint.iacr.org/2014/140.pdf , (2014)

[8] ”Elliptic curve point multiplication”, 2014.
http://en.wikipedia.org/wiki/Elliptic_curve_point_multiplication , (2014.)

Sažetak

U ovom radu smo definirali zbrajanje i multiplikaciju točaka na eliptičkim krivuljama, te proučavali složenosti istih operacija u različitim koordinatama. U prvom poglavlju smo definirali osnovne algebarske pojmove nužne za razumijevanje ostatka rada, specifično grupe, prstenove i polja. U drugom poglavlju smo definirali pojam eliptičke krivulje, te zbrajanje točaka i množenje skalarom. U trećem poglavlju smo obavili centralni dio ovog diplomskog rada, pokazali prikaz eliptičke krivulje u različitim koordinatnim sustavima, te analizirali složenost zbrajanja i multiplikacije skalarom.

Summary

In this work we have defined addition and multiplication of points on elliptic curves and analysed complexity of said operations in different coordinates. First chapter was about defining basic algebraic notions necessary for understanding the rest of the work, those notions being groups, rings and fields. In second chapter we have defined the concept of elliptic curves along with point addition and scalar multiplication. Third chapter is the main part of this work. In it we have shown equation of elliptic curves in different coordinates and have analysed different complexities of addition and scalar multiplication.

Životopis

Rođen sam 16. veljače 1986. godine u Bjelovaru. Upisujem 3. osnovnu školu u Bjelovaru 1992. godine, zbog selibe se 1993. godine prebacujem u 2. osnovnu školu u Bjelovaru. Za vrijeme osnovne škole bavim se rukometom i plivanjem. Upisujem matematičku gimnaziju u Bjelovaru 2000. godine. Za vrijeme srednje škole bavim se atletikom s nekoliko osvojenih medalja na regionalnim natjecanjima. Godine 2004. završavam gimnaziju te polažem maturu s odličnim uspjehom te iste godine upisujem Prirodoslovno-matematički fakultet u Zagrebu. Sudjelujem na nekoliko međufakultetskih natjecanja u trčanju. Godine 2011. upisujem Diplomski sveučilišni studij Računarstva i matematike. Aktivno se bavim plesom.