Kriptografija eliptičkih krivulja s pogledom prema kvantnom računarstvu

Solo, Loris

Sveučilište Jurja Dobrile u Puli
Tehnički fakultet u Puli

Loris Solo

Kriptografija eliptičkih krivulja s pogledom prema kvantnom računarstvu

Završni rad

Pula, rujan, 2023. godine

Sveučilište Jurja Dobrile u Puli
Tehnički fakultet u Puli

Loris Solo

Kriptografija eliptičkih krivulja s pogledom prema kvantnom računarstvu

Završni rad

JMB:0069086486, redoviti student

Studijski smjer: Računarstvo

Predmet: Matematika 1, Matematika 2
Znanstveno područje: 1. Područje prirodnih znanosti
Znanstveno polje: 1.01. Matematika
Znanstvena grana: 1.01.01 algebra, 1.01.02 geometrija i topologija, 1.01.05 matematička logika i računarstvo
Mentor: Neven Grbac

Pula, rujan, 2023. godine

Tehnički fakultet u Puli

Ime i prezime studenta Loris Solo
JMBAG 0069086486

Status: ☒ redoviti ☐ izvanredni

PRIJAVA TEME ZAVRŠNOG RADA

Neven Grbac
Ime i prezime mentora

Računarstvo
Studij

Matematika 1, Matematika 2
Kolegij

Potvrđujem da sam prihvatio/la temu završnog/diplomskog rada pod naslovom:
Kriptografija eliptičkih krivulja s pogledom prema kvantnom računarstvu

(na hrvatskom jeziku)

Elliptic Curve Cryptography in View of Quantum Computing

(na engleskom jeziku)

Datum: 21.3.2023.

IZJAVA O KORIŠTENJU AUTORSKOGA DJELA

Ja, **Loris Solo**, dajem odobrenje Sveučilištu Jurja Dobrile u Puli, nositelju prava korištenja, da moj završni rad pod nazivom „Kriptografija eliptičkih krivulja s pogledom na kvantno računarstvo“ upotrijebi da tako navedeno autorsko djelo objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te preslika u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu sa Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

Potpis

U Puli, 28.8.2023

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani **Loris Solo**, kandidat za prvostupnika računarstva ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

Solo

U Puli, 28.8.2023 godine

Sadržaj:

1. Uvod

Predmet istraživanja odnosno tema ovog rada je kriptografija eliptičkih krivulja s pogledom prema kvantnom računarstvu. Naglasak se stavlja na objašnjenje eliptičkih krivulja kroz jednostavne primjere te grafičke prikaze.

Cilj rada je povezati kriptografiju i eliptičke krivulje koje se smiju koristiti u kriptografiji, a svrha rada je istaknuti važnost matematičkih operacija koje se mogu izvoditi na eliptičkim krivuljama, a koje imaju značaj za kriptografiju.

Struktura rada prati strukturu lijevka budući da se od općenitog ide prema konkretnijem. Prvo se teorijski objašnjavaju pojmovi nužni za razumijevanje teksta, a nakon toga se prikazuje praktičan primjer. Rad započinje definiranjem i podjelom kriptografije. Nakon toga, prelazi se na definiranje eliptičkih krivulja pri čemu se objašnjavaju njihovi izgledi i varijante. Nadalje, govori se o matematičkim operacijama nad krivuljama, zašto su one važne te koje se krivulje smiju koristiti u kriptografske svrhe. Pri kraju rada iskazan je utjecaj kvantnih računala na kriptografske sustave koji se trenutno koriste, a rad završava iznošenjem zaključka i prikazom literature te popisom slika i tablica.

2. Kriptografija

Kriptografija je znanstvena disciplina koja se bavi pronalaženjem novih tehnika zaštite podataka sa svrhom omogućavanja sigurnijeg prijenosa podataka tako da isti ostanu nerazumljivi osobama kojima nisu namijenjeni. Prvi znakovi kriptografije pronađeni su u Egiptu, a datiraju iz 1900. godine prije Krista što ukazuje da je razvoj kriptografije započeo puno prije postojanja računala [3].

Cezarova šifra jedna je od najpoznatijih i najjednostavnijih šifri u kriptografiji, a naziv je dobila po Gaju Juliju Cezaru. Cezarova šifra bazira se na principu zamjene slova običnog teksta s drugim slovom abecede koje je u abecednom redu udaljeno za onoliko mjesta udesno koliko je to prethodno dogovoreno. Primjerice (slika 1), odredi li se da će se slovo A zamijeniti slovom koje je udaljeno za 5 mjesta udesno, tada će se umjesto slova A koristiti slovo D, umjesto slova B slovo DŽ i tako dalje do kraja abecede [4].

Slika 1 prikaz promjene slova šifriranih Cezarovom šifrom:

Izvor: obrada podataka

Razvojem računala pojavile su se nove vrste kriptografije. Stoga se danas kriptografija dijeli na kriptografiju tajnog ključa (eng. *secret key cryptography*) i kriptografiju javnog ključa (eng. *public key cryptography*), odnosno simetričnu i asimetričnu kriptografiju.

2.1 Simetrična enkripcija

Simetrična enkripcija koristi samo jedan ključ za šifriranje i dešifriranje podataka što ju čini bržom i jednostavnijom od asimetrične enkripcije koja, pak, koristi dva ključa. Dakle, entiteti koji razmjenjuju podatke prethodno trebaju razmijeniti ključ za dešifriranje istih. Upravo ta razmjena ključa predstavlja problem simetrične enkripcije budući da treba pronaći najsigurniji način prijenosa ključa od Alice do Boba. Ako se ključ, primjerice pošalje E-mailom tada se on može presresti i koristiti za dešifriranje podataka od strane neovlaštene osobe. Kako bi se spriječio navedeni problem osmišljena je asimetrična enkripcija.

Tipovi algoritama simetrične enkripcije mogu se podijeliti na blok algoritme i stream algoritme.

Blok algoritmi, kako i sam naziv kaže, šifriraju podatke u blokovima podataka pri čemu se svaki blok šifrira istim ključem. To znači da će isti blok podataka šifriran istim ključem uvijek dati isti rezultat. Drugim riječima, isti običan tekst koji se šifrira istim ključem dati će isti šifrirani tekst, a to predstavlja ranjivost. Navedeni primjer je najkorišteniji i najjednostavniji način rada blok algoritama, a naziva se *Electronic Codebook* (ECB) [3].

Jedan od načina rada je i *Cipher Block Chaining* (CBC) pri kojemu se dva ista podatka neće šifrirati u iste šifrirane podatke jer CBC ima povratnu vezu s procesom šifriranja tako da se obavlja isključivo ILI (XOR) operacija između običnog teksta i teksta koji se šifrirao u prijašnjem koraku [3].

Stream algoritmi vrše svoje operacije na samo jednom bitu istovremeno te se od glavnog tajnog ključa stvaraju podključevi koji kriptiraju podatke tako da se svaki podatak kriptira različitim podključem, čime se osigurava da se dva ista podatka ne šifriraju nužno u iste šifrirane podatke [3].

Algoritmi simetrične enkripcije:

- *Blowfish*
- *Data Encryption Standard* (DES)
- *Advanced Encryption Standard* (AES)

2.2 Asimetrična enkripcija

Asimetrična enkripcija koristi dva ključa od kojih je jedan javni ključ (eng. *public key*), a drugi privatan ključ (eng. *private key*). Najčešće korišteni algoritam asimetrične enkripcije je RSA (Rivest, Shamir, Adleman) [17] algoritam koji generira privatni i javni ključ, a oni su matematički povezani. No, iako povezani, ne može se dobiti privatni ključ uz poznavanje samo javnog ključa. Javni ključevi se koriste za šifriranje podataka, a podaci se mogu dešifrirati samo privatnim ključem. Kako bi dvije osobe mogle komunicirati prvo moraju razmijeniti svoje javne ključeve. Zatim se podaci šifriraju s navedenim javnim ključevima i povratno šalju vlasnicima javnog ključa koji tada dešifriraju podatke pomoću privatnog ključa. U slučaju da treća osoba (Eve) ukrade privatni ključ od Alice, ona će imati pristup isključivo podacima koji pristižu Alice, ali ne i onima koje Alice šalje drugim osobama.

3. Eliptičke krivulje

Eliptičke krivulje mogu se definirati kao skup točaka u polju K koje zadovoljavaju jednadžbe oblika:

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

gdje su a_1, a_2, a_3, a_4, a_6 koeficijenti iz odgovarajućeg polja. Kako bi ova jednadžba predstavljala eliptičku krivulju nužno je zadovoljiti uvjet da je u svakoj točki barem jedna parcijalna derivacija različita od nule [2].

U slučajevima kada je karakteristika polja K različita od dva i tri, opći se oblik može transformirati u kratku Weierstrassovu formu pa se može reći da je eliptička krivulja E nad poljem K kubna nesingularna krivulja koja se sastoji od točaka (x, y) koje zadovoljavaju jednadžbu oblika:

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

zajedno s elementom $\mathcal{O}$ koji se naziva „točka u beskonačnosti“ [1].
Kako bi se osiguralo da krivulja nije singularna moraju se zadovoljiti zahtjevi da diskriminanta $\Delta = -4a^3 - 27b^2$ nije 0 odnosno da polinom $x^3 + ax + b$ nema višestrukih nultočaka [2].

3.1 Eliptičke krivulje za realne brojeve

Eliptičke krivulje nad poljem realnih brojeva su algebarske krivulje oblika:

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

.

gdje (a, b) predstavlja par realnih brojeva, a predznak diskriminante $4a^3 + 27b^2 \neq 0$ određuje broj komponenta koje krivulja ima. Ako je $4a^3 + 27b^2 < 0$ (slika 2), krivulja ima jednu komponentu, a ako je $4a^3 + 27b^2 > 0$, tada krivulja ima dvije komponente (slika 3).

Primjer 3.1.1:

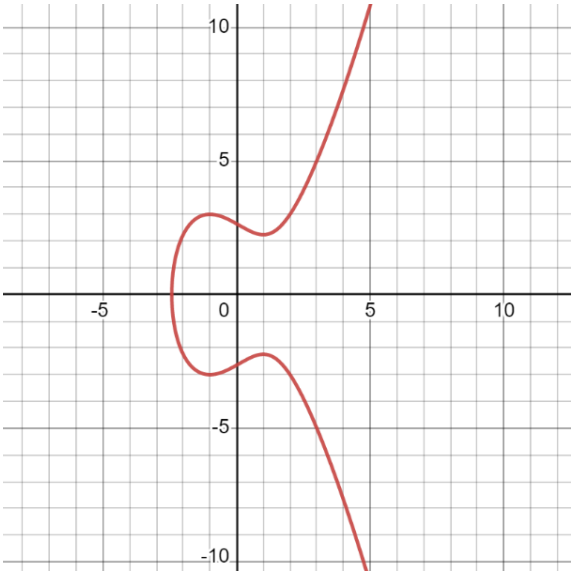
Krivulja 1: $y^2 = x^3 - 3x$

Krivulja 2: $y^2 = x^3 - 3x + 7$

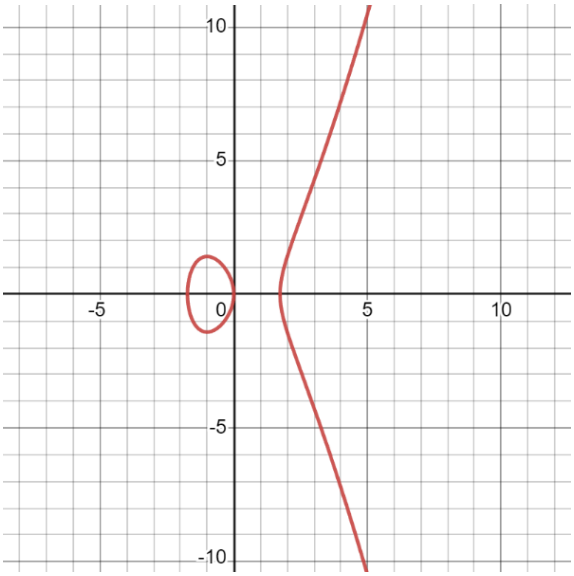
$$\Delta_1 = 4 * (-3)^3 = -108$$

$$\Delta_2 = 4 * (-3)^3 + 27 * 7^2 = 1215$$

Slika 2 krivulja 1



Slika 3 krivulja 2



Izvor: obrada podataka

Zakon grupe na eliptičkim krivuljama predstavlja način zbrajanja dviju točaka na krivulji kako bi se dobila treća točka koja također leži na krivulji.

Pod pretpostavkom da su točke P i Q različite točke koje se nalaze na eliptičkoj krivulji E, želi se pronaći treća točka $-R$ koja leži na pravcu koji prolazi kroz P i Q.

Pravac će presijecati krivulju u jedinstvenoj trećoj točki, odnosno točki koja se naziva $-R$.

Ako su P i Q jedna te ista točka ($P + P$), tada se povlači tangenta na krivulju u toj točki i pronalazi se sjecište s krivuljom. To sjecište je jedinstveno i naziva se točka $-2P$ (slika 4).

Zakon grupe se definira tako da je zbroj dviju točaka P i Q osnosimetrična slika točke $-R$ $(-2P)$ u odnosu na x-os. Simbolički se piše:

$$P + Q = R$$
$$P + P = R = 2P$$

pri čemu je točka R refleksija $-R$ $(-2P)$ u odnosu na x-os (slike 4,5).
Točka u beskonačnosti označena s $\mathcal{O}$ je neutralni element grupe. Drugim riječima, za bilo koju točku P na krivulji vrijedi:

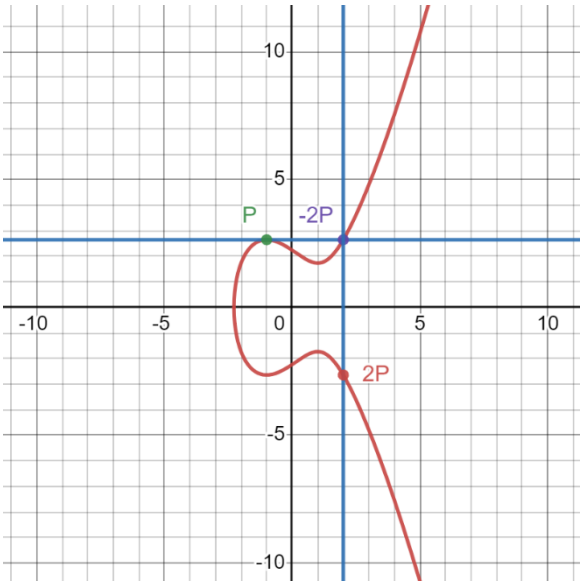
$$P + \mathcal{O} = P$$

i

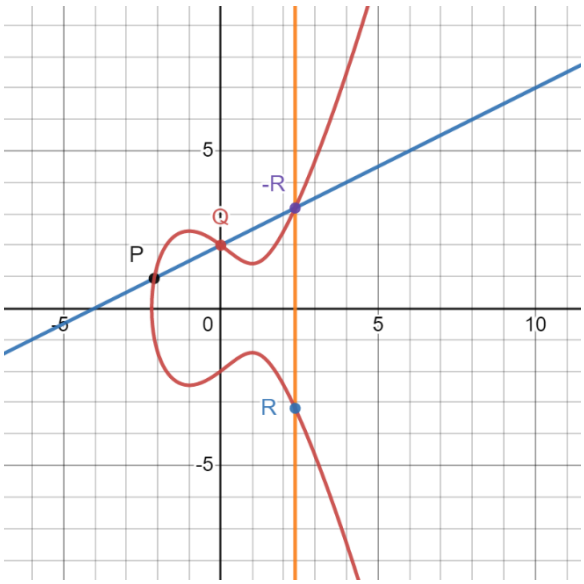
$$\mathcal{O} + P = P$$

Zakon grupe eliptičkih krivulja, definiran gore, zaista ima svojstva koja ga čine komutativnom grupom, a to su asocijativnost, postojanje neutralnog elementa, postojanje inverznih elemenata i komutativnost. Ova komutativna grupa naziva se grupa eliptičke krivulje nad realnim brojevima i važna je u kriptografiji.

Slika 4 grafički prikaz zbroja iste točke na krivulji



Slika 5 grafički prikaz zbroja 2 različite točke na krivulji



Izvor: obrada podataka

Točka R se osim na geometrijski način može pronaći i algebarski tako da se prvo nađe nagib s pravca koji ide kroz točke P i Q.

$$s = \frac{y_P - y_Q}{x_P - x_Q}$$

Zatim se nađu koordinate x i y točke R pomoću sljedećih formula:

$$x_R = s^2 - (x_P + x_Q)$$
$$y_R = s * (x_P - x_R) - y_P$$

Primjer 3.1.2: Eliptička krivulja E zadana je jednadžbom $y^2 = x^3 - 3x + 5$. Pravac y zadan je jednadžbom $y = x + 2$ koji sječe krivulju E u točkama: $P(-2.273, -0.273)$ i $Q(0.14, 2.14)$.

Korištenjem formule za nagib pravca ispostavi se da je nagib pravca 1.

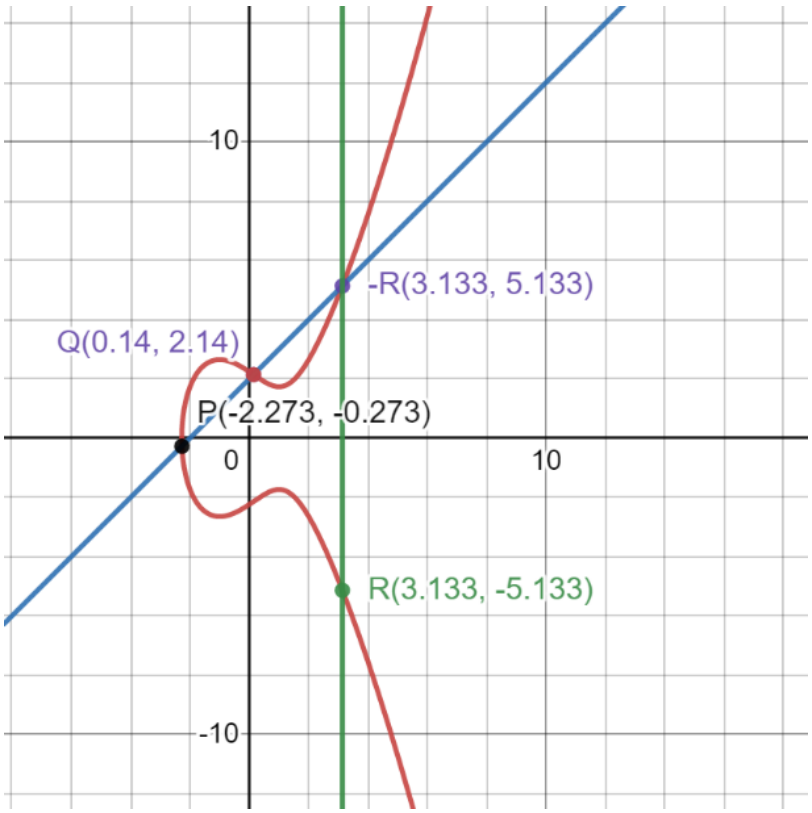
$$s = \frac{-0.273 - 2.14}{-2.273 - 0.14} = 1$$

Nakon izračunavanja nagiba pravca preostaje još pronalaženje koordinata točke $R(3.133, 5.133)$. Također, za izračunavanje ovih koordinata koriste se prethodno spomenute formule.

$$x_R = 1^2 - (-2.273 + 0.14) = 3.133$$
$$y_R = 1 * (-2.273 - 3.133) - (-0.273) = -5.133$$

Izračun se može provjeriti grafički (slika 6)

Slika 6 grafička provjera izračuna



Izvor: obrada podataka

U slučaju da su točke P i Q ista točka $(P + P)$, točka R se na algebarski način može pronaći pomoću sljedećih formula:

$$s = \frac{3{x_p}^2 + a}{2y_p}$$

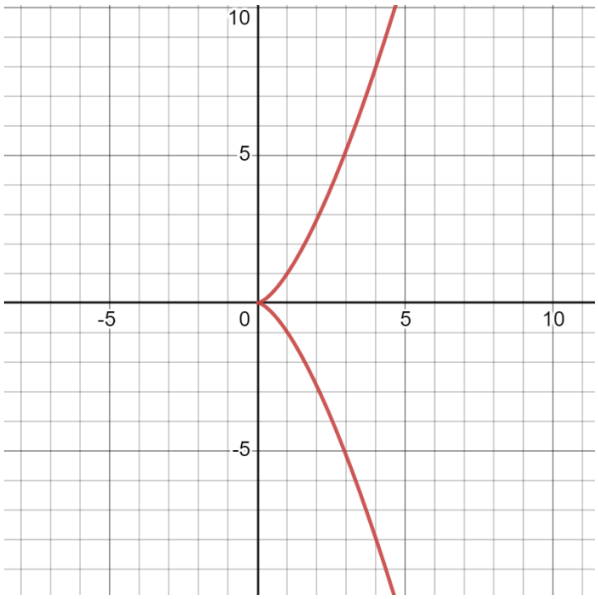
$$x_R = s^2 - 2x_P$$

$$y_R = s(x_P - x_R) - y_P$$

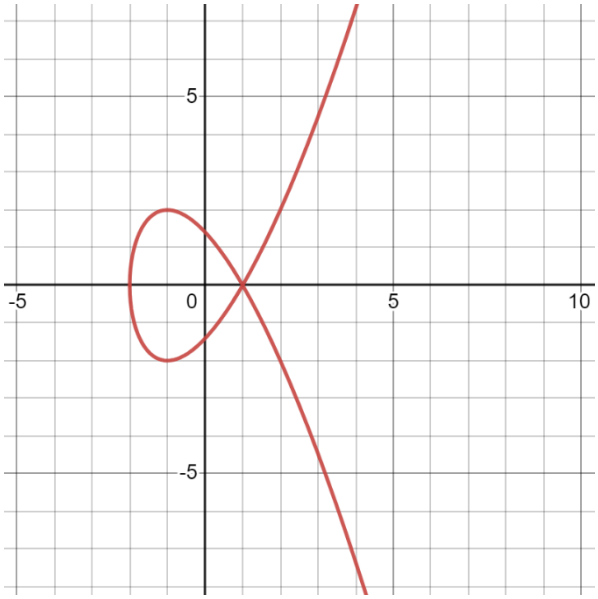
3.2 Singularne eliptičke krivulje

Eliptička krivulja je singularna ako postoji barem jedna točka na krivulji u kojoj krivulja nije „glatka“, što može značiti da krivulja ima kasp (slika 7) [14] ili samosjecište (slika 8) [14] u nekoj točki.

Slika 7 $y^2 = x^3$



Slika 8 $y^2 = x^3 - 3x + 2$



Izvor: autor modificirao

Singularne eliptičke krivulje ne koriste se u kriptografiji budući da one mogu uvesti ranjivosti i potencijalne slabosti. Singularne eliptičke krivulje kompliciraju aritmetičke operacije koje su temeljne za kriptografiju eliptičke krivulje (ECC). U ECC-u, šifriranje, dešifriranje i generiranje ključeva oslanjaju se na operacije zbrajanja i množenja točaka. Ove operacije postaju složenije i manje učinkovite kada se radi o singularnim krivuljama.

4. Eliptičke krivulje koje se smiju koristiti u kriptografiji

Kriptografija eliptičke krivulje (eng. Elliptic Curve Cryptography, ECC) uključuje odabir krivulja koje će se koristiti u kriptografske svrhe, a postoje brojni standardi koji daju smjernice za navedeni proces odabira. Drugim riječima, postoji više skupina pravila ili preporuka za odabir odgovarajućih krivulja za korištenje u ECC-u. U nastavku su navedeni neki od njih:

- ANSI X9.62 (1999).
- IEEE P1363 (2000).
- SEC 2 (2000).

- NIST FIPS 186-2 (2000).
- ANSI X9.63 (2001).
- Brainpool (2005).
- NSA Suite B (2005).

Svaki standard nastoji osigurati da problem diskretnog logaritma eliptičke krivulje (ECDLP) bude što teži, ali povećanje težine diskretnog logaritma neće uvijek učiniti ECC sigurnijom. Ukratko, ECDLP je problem pronalaženja tajnog ključa ECC korisnika obzirom na javni ključ korisnika, no o tome će biti detaljnije kasnije u tekstu. Postoje slučajevi kada je kriptografija eliptičkih krivulja bila probijena bez rješavanja problema diskretnog logaritma. Najveći problem predstavlja pogrešna implementacija kriptografije eliptičkih krivulja budući da takva implementacija za posljedice ima: propuštanje tajnih podataka kroz vrijeme predmemorije ili vrijeme grananja, propuštanje tajnih podataka kad unos nije točka na krivulji te mogućnost davanja krivih rezultata za neke rijetke točke krivulje. [5]

Neki od nedostataka temeljeni na razlikama između ECDLP-a i stvarnog ECC-a koje napadači mogu iskoristiti su to što je ECDLP neinteraktivan dok ECC u stvarnom svijetu obrađuje unose koje kontrolira napadač. Nadalje, ECDLP otkriva samo nP, a ECC u stvarnom svijetu može otkriti više informacija sporednih kanala. Također, dok ECDLP uvijek ispravno izračunava nP, kod ECC u stvarnom svijetu povremeno se događaju kvarovi $[5]$.

Većina tih napada bila bi spriječena boljim izborom krivulja koje bi omogućile sigurnije i jednostavnije implementacije.
Postoji teoretska mogućnost implementacije sigurnih verzija standardnih krivulja, ali to je veoma složen zadatak [5].

4.1 Duljina ključa

Kriptografija eliptičke krivulje oslanja se na dva glavna parametra: eliptičku krivulju E nad pogodnim konačnim poljem i određenu točku G na E poznatu kao bazna točka (generator). Bazna točka ima u grupi eliptičke krivulje nad odabranim poljem određeni red, označen s n, što predstavlja veliki prosti broj, koji je ujedno i red podgrupe generirane s G. Ukupan broj točaka na krivulji jednak je h pomnoženom s n, gdje je h cijeli broj koji se naziva kofaktor i nije djeljiv s n. Za učinkovitost je važno da kofaktor bude što je moguće manji, a po mogućnosti jednak jedan [6].

Kako bi se osiguralo da su privatni i javni ključevi generirani kriptografijom eliptičke krivulje približno iste duljine, potrebno je da krivulje koje se koriste imaju kofaktor 1, 2, 4 ili 8 [6].

4.2 Izbor temeljnih polja

Za svaku duljinu ključa dostupne su dvije vrste polja:

- Konačno polje, označeno kao F_p, sadrži prosti broj p elemenata. Svaki element u ovom polju je cijeli broj koji se uzima po modulu p. Aritmetičke operacije izvode se pomoću aritmetike cijelih brojeva koji se, također uzimaju po modulu p [6].

- Binarno polje, označeno kao F_{2^m}.Polje sadrži 2^m elemenata, gdje je m stupanj polja. Elementi u ovom polju su nizovi bitova duljine m, a aritmetičke operacije se provode pomoću operacija na samim bitovima [6].

Tablica 1 daje približne razine sigurnosti za navedene eliptičke krivulje. Razina sigurnosti eliptičke krivulje izravno je povezana s redom, odnosno podgrupom njezine bazne točke. Ako eliptička krivulja ima baznu točku određenog reda n, razina sigurnosti koju pruža krivulja može se grubo procijeniti kao polovica broja bitova od n. [6].

Tablica 1. Razine sigurnosti za različite krivulje

Razina sigurnosti	Preporučene krivulje
112	P-224, K-233, B-233
128	P-256, W-25519, Curve25519, Edwards25519, K-283, B-283
192	P-384, K-409, B-409
224	W-448, Curve448, Edwards448, E448
256	P-521, K-571, B-571

Izvor: NIST Special Publication NIST SP 800-186 Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters Eliptic Curve Cryptography An Implementation tutorial

4.3 P-224

Eliptička krivulja P-224 je krivulja Weierstrassovog tipa. Definirana je nad prostim poljem F_p s $p = 2^{224} - 2^{96} + 1$ elemenata.

Parametri domene[1]:

p

$= 26959946667150639794667015087019630673557916260026308143510066298881$

$h = 1$

n

$= 26959946667150639794667015087019625940457807714424391721682722368061$

$a = -3$

b

$= 18958286285566608000408668544493926415504680968679321075787234672564$

x_G

$= 19277929113566293071110308034699488026831934219452440156649784352033$

y_G

$= 19926808758034470970197974370888749184205991990603949537637343198772$

[1] Parametri domene preuzeti su iz NIST Special Publication NIST SP 800-186 Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters
Eliptic Curve Cryptography An Implementation tutorial, str 10

5. Eliptičke krivulje nad konačnim poljima

Eliptička krivulja nad konačnim poljem F_p definirana je jednadžbom:

$$y^2 \, mod \, p = x^3 + ax + b \, mod \, p,$$

gdje je p prosti broj, a elementi konačnog polja su cijeli brojevi $\{0,1,2 \dots p-1\}$. Važno je istaknuti: $4a^3 + 27b^2 \, mod \, p \neq 0$. Da bi se osigurala sigurnost kriptosustava, prosti broj p mora biti odabran tako da postoji konačan broj točaka na eliptičkoj krivulji. Krivulje koje specificira *Standards for efficient cryptoraphy* (SEC) imaju p u rasponu između 112-521 bita.

Budući da graf ove jednadžbe eliptičke krivulje nije gladak, geometrijsko objašnjenje zbrajanja i udvostručavanja točaka, kao u realnim brojevima, nije primjenjivo. Međutim, algebarska pravila za zbrajanje i udvostručenje točaka mogu se prilagoditi za eliptičke krivulje nad F_p. Sve aritmetičke operacije, uključujući zbrajanje, oduzimanje, množenje i dijeljenje, izvode se pomoću cijelih brojeva između 0 i $p-1$ te modularne aritmetike modula p.

Primjer 4.0.1: U svrhu određivanja točaka krivulje E koja je zadana jednadžbom: $y^2 = x^3 - 3x + 4$ nad poljem F_7 (slika 9) potrebno je poznavati potpune kvadrate $mod \, 7$. Potpuni kvadrati su :

$$(\pm 0)^2 = 0, (\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 = 9 \, mod \, 7 = 2$$

Uvrštavanjem x koordinata u jednadžbu i računanjem dobije se sljedeća tablica:

Tablica 2. Izračun točaka eliptičke krivulje

x	x^2	$x^3 - 3x + 4$	y	**TOČKE**
0	0	4	2,5	(0,2), (0,5)
1	1	2	3,4	(1,3), (1,4)
2	4	6	/	/
3	2	1	1,6	(3,1), (3,6)
4	2	0	0	(4,0)
5	4	2	3,4	(5,3), (5,4)
6	1	6	/	/

Izvor: obrada podataka

Iz tablice se može iščitati sljedeće:

$$E(F_7) = \{\mathcal{O}, (0,2), (0,5), (1,3), (1,4), (3,1), (3,6), (4,0), (5,3), (5,4)\}$$

Za izračun zbroja dvije točke na $E(F_7)$, na primjer $P(3,6)$ i $Q(5,4)$, prvo je potrebno izračunati nagib pravca s kroz te dvije točke:

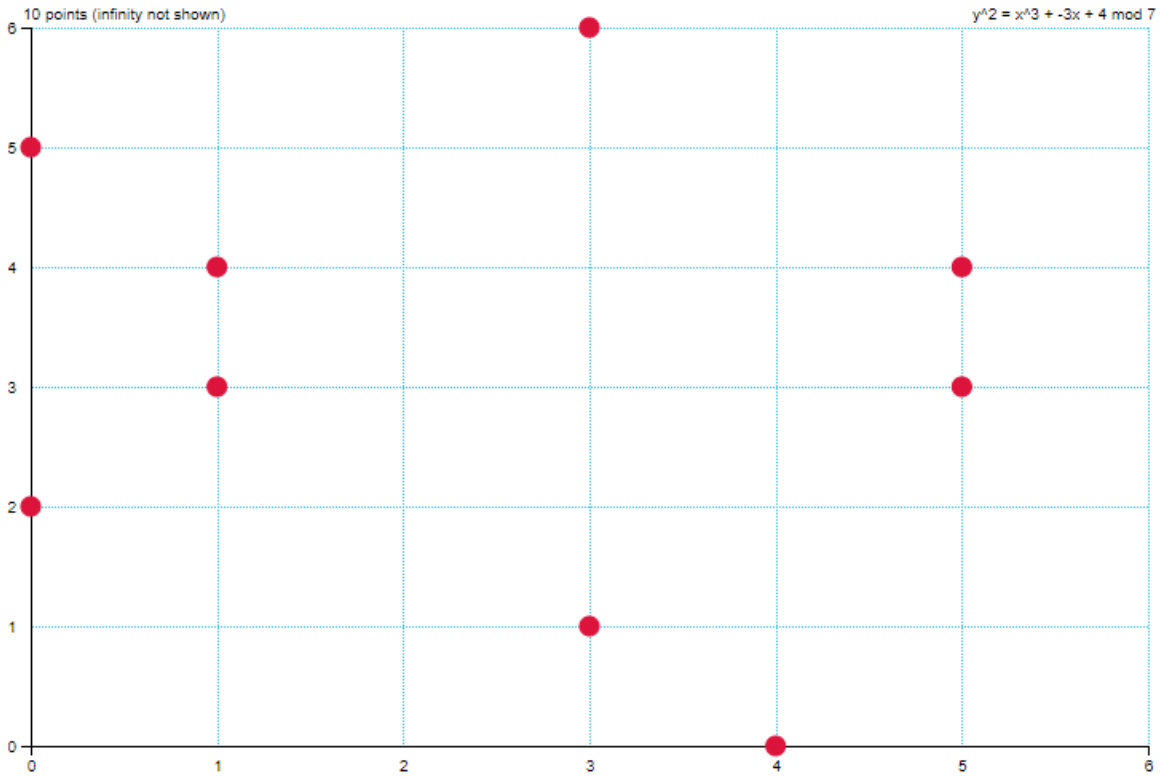
$$s = \frac{y_P - y_Q}{x_P - x_Q} = \frac{6-4}{3-5} \equiv 6 \; mod \; 7$$

Tada je:

$$x_R = s^2 - x_P - x_Q = 36 - 3 - 5 \equiv 0 \; mod \; 7,$$
$$y_R = s(x_P - x_R) - y_P = 6(3-0) - 6 \equiv 5 \; mod \; 7.$$

Ovime se dobije da je $(3,6) + (5,4) = (0,5)$.

Slika 9 eliptička krivulja nad konačnim poljem



Izvor: obrada podataka

6. Problem diskretnog logaritma eliptičkih krivulja

Problem diskretnog logaritma jedan je od temeljnih problema na kojima se temelji kriptografija. Teško je rješiv, ali se lako provjerava.

Problem glasi: „Zadana je eliptička krivulja E nad konačnim poljem F_p i dvije točke G i Q na krivulji. Treba pronaći cijeli broj n tako da je $Q = nG$, gdje nG označava dodavanje G samom sebi n puta“ [15].

Težina rješavanja problema očituje se u nepostojanju učinkovitog algoritma za rješavanje ovog problema, ali za zadani n lako je provjeriti je li $Q = nG$ dodavanjem G samom sebi n puta i provjerom dobije li se Q.

Primjer 5.0.1: Potrebno je pronaći diskretni logaritam n točke $Q = (3,6)$ obzirom na baznu točku $G = (1,7)$, ako je zadana eliptička krivulja $y^2 = x^3 + 23x + 42$ nad poljem F_{17}.

Jedan od načina za pronalaženje n je izračunavanjem višekratnika G sve dok se ne pronađe pravi Q.

$$G(1,7)$$

$$s = \frac{3{x_1}^2 + a}{2y_1} = \frac{3 * 1^2 + 23}{14} \equiv \frac{26}{14} \ mod\ 17 \ \equiv \ \frac{9}{14} \ mod\ 17$$

Za izračun $\frac{9}{14} \ mod\ 17$, može se iskoristiti činjenica da je dijeljenje u konačnom polju definirano kao množenje modularnim inverzom djelitelja.

Za dobivanje modularnog inverza koristi se Euklidov algoritam:

$$17 = 1 * 14 + 3$$

$$14 = 4 * 3 + 2$$

$$3 = 1 * 2 + 1$$

Unatrag:

$$1 = 3 - 1 * 2$$

$$1 = 3 - 1(14 - 4 * 3)$$

$$1 = -1 * 14 + 5 * 3$$

$$1 = -1 * 14 + 5 * (17 - 14)$$

$$1 = 5 * 17 - 6 * 14$$

Dobije se da je modularni inverz od 14 u polju F_{17} jednak -6 odnosno 11.

Nadalje se dobije:

$$\frac{9}{14} \ mod\ 17 = 9 * 11 \ mod\ 17$$

$$= 99 \ mod\ 17$$

$$s = 14$$

Nakon dobivanja nagiba s mogu se izračunati koordinate:

$$x_2 = s^2 - 2x_1 = \ 14^2 - 2 - 1 \equiv 194 \ mod\ 17 \equiv 7$$

$$y_2 = s(x_1 - x_2) - y_1 = 14(1 - 7) - 7 \equiv -91 \ mod\ 17 \ \equiv 11$$

$$2G = (7,11)$$

Budući da točka $2G$ nije Q potrebno je izračunati točku $3G$ i tako dalje sve dok ne dobijemo:

$$nG = Q$$

Izračun $3G$. Obzirom da je $3G = G + 2G$ vrijedi:

$$s = \frac{y_2 - y_1}{x_2 - x_1} = \frac{11 - 7}{7 - 1} \equiv \frac{4}{6}\ mod\ 17$$

$$s = 12$$

$$x_3 = s^2 - x_2 - x_1 = 12^2 - 1 - 7 \equiv 136\ mod\ 17 \equiv 0$$

$$y_3 = s(x_1 - x_3) - y_1 = 12(1 - 0) - 7 \equiv 5$$

$$3G = (0,5)$$

Izračun $4G$. Obzirom da je $4G = G + 3G$ vrijedi:

$$s = \frac{y_3 - y_1}{x_3 - x_1} = \frac{5 - 7}{0 - 1} \equiv 2$$

$$x_4 = s^2 - x_3 - x_1 = 2^2 - 0 - 1 \equiv 3$$

$$y_4 = s(x_1 - x_4) - y_1 = 14(1 - 3) - 7 \equiv -11\ mod\ 17 \equiv 6$$

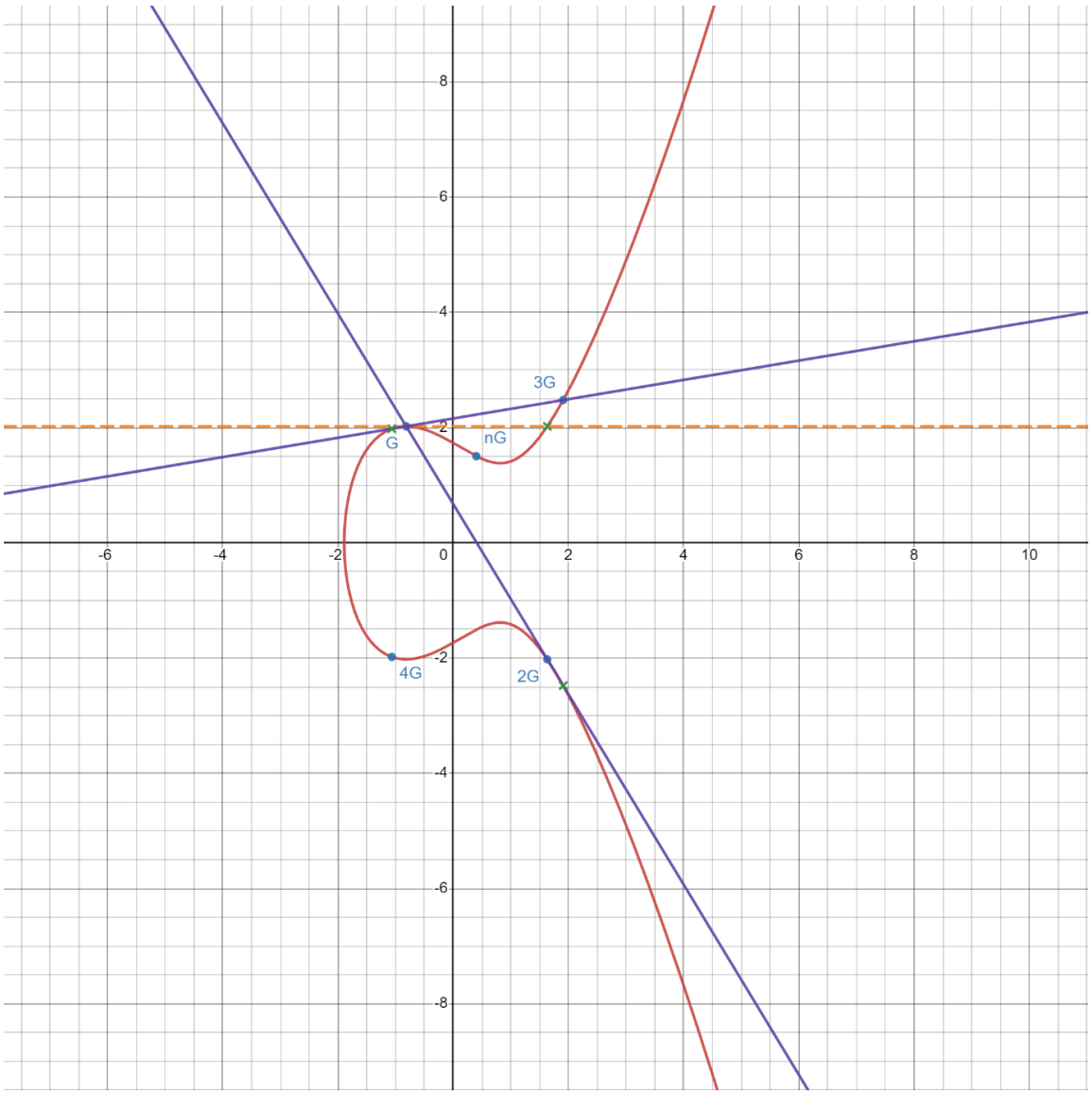
$$4G = (3,6)$$

Budući da je $4G = (3,6) = Q$, diskretni logaritam od Q s obzirom na baznu točku G je $n = 4$.

U praktičnim kriptografskim primjenama odabrala bi se dovoljno velika vrijednost n da bi vrijednost iste bilo neizvedivo odrediti ovakvom direktnom metodom „grube sile“.

Sljedeća slika (slika 10) prikazuje eliptičku krivulju $y^2 = x^3 - 2x + 3$ iz primjera nad realnim poljem (zbog lakšeg razumijevanja), te grafički prikazuje prve 4 točke koju su dobivene od točke G. Svrha slike je slikovito prikazati problem diskretnog logaritma eliptičkih krivulja odnosno da je jedini način za saznanje vrijednost n u točki nG kretanje po grafu (zbrajanje točaka) sve dok se ne dođe do točke $nG = Q$.

Slika 10 prikaz problema diskretnog logaritma eliptičke krivulje



Izvor: obrada podataka

7. Diffie-Hellmanov protokol

Diffie-Hellmanova razmjena ključeva omogućuje dvjema stranama stvaranje zajedničkog tajnog ključa u suradnji, čak i kada komuniciraju preko nesigurnog kanala [1] [8]. Kako bi razmjena ključeva bila što sigurnija preporučuju se ključevi od 2048 bitova ili veći [13]. Primjerice, dvoje ljudi (Alice i Bob) žele komunicirati na javnoj mreži, a Eve želi saznati njihove podatke. Kako bi onemogućili presretanje podataka, Alice i Bob moraju stvoriti zajednički tajni ključ tako da[2]:

[2] Ovaj opis protokola je preuzet iz Shevchuk, O. *Introduction to elliptic curve cryptography, 2020, str. 3*

1. Alice odabere svoj nasumični broj α po kriteriju:
$$1 \leq \alpha \leq p-1$$
i računa $l = g^{\alpha} \, mod \, p$ kojeg šalje Bobu.
2. Bob odabere svoj nasumični broj β po kriteriju:
$$1 \leq \beta \leq p-1$$
i računa $m = g^{\beta} \, mod \, p$ kojeg šalje Alice.
3. Alice uzme Bobov javni rezultat m i podiže ga za potenciju svog privatnog broja dobivajući $m^{\alpha} \, mod \, p$.
4. Bob uzme javni rezultat l od Alice i podiže ga za potenciju svog privatnog broja dobivajući $l^{\beta} \, mod \, p$.
5. Primjećuje se da je $m^{\alpha} \, mod \, p = (g^{\beta})^{\alpha} \, mod \, p = (g^{\alpha})^{\beta} \, mod \, p = l^{\beta} \, mod \, p = s$ odnosno zajednički ključ.

Budući da su α i β privatni ključevi, Eve ima pristup samo javnim podacima l, m, g, p te mora saznati $g^{\alpha\beta} \, mod \, p$ poznavajući samo te podatke. Izračun $g^{\alpha\beta} \, mod \, p$ poznavajući samo javne podatke je računski gotovo neizvedivo zbog problema diskretnog logaritma. Ako je p iznimno velik ni najjača računala ne mogu pronaći α poznavajući samo javne podatke tako da vrijedi $g^{\alpha} = l \, mod \, p$ [1]. Nadalje, korištenje generatora g dodatno otežava problem za Evu budući da potencije g mogu biti bilo koji element u polju čime se povećavaju mogući izbori privatnih ključeva α i β.

Primjer 6.0.1: Alice i Bob javno se dogovore oko generatora g = 5 i osnovnog modula p = 23.

Stvaranje ključa:

1. $\alpha = 7, l = 5^{7} mod \, 23 = 78125 \, mod \, 23 = 17$
2. $\beta = 3, m = 5^{3} = 125 \, mod \, 23 = 10$
3. $m^{\alpha} \, mod \, p \rightarrow 10^{7} \, mod \, 23 = 14$
4. $l^{\beta} \, mod \, p \rightarrow 17^{3} \, mod \, 23 = 14$
5. $10^{7} \, mod \, 23 = (5^{3})^{7} \, mod \, 23 = (5^{7})^{3} \, mod \, 23 = 17^{3} \, mod \, 23 = 14$

7.1 Diffie-Hellmanov protokol za eliptičke krivulje

Isto kao i kod običnog Diffie-Hellmanovog protokola Alice i Bob žele sigurno komunicirati na nesigurnoj mreži [8]. Kako bi to bilo moguće Alice i Bob moraju se dogovoriti oko javnih podataka (p, a, b, G, n, h), odnosno parametara domene.

- p – prost broj za koji promatramo polje ($mod\ p$)
- a, b – parametri eliptičke krivulje
- G – bazna točka (generator)
- n – red od G, odnosno red podgrupe generirane s G
- h - kofaktor

Primjer 6.0.2: Zadana je krivulja iz primjera **5.0.1** $y^2 = x^3 + 23x + 42\ mod\ 17$ s istom baznom točkom $G(1,7)$. Nakon što se zna bazna točka potrebno je izračunati cikličku grupu za tu točku (izračun prvih 4 točaka prikazan je u primjeru **5.0.1**).
Ciklička grupa:

$$G = (1,7) \qquad 8G = (9,3)$$

$$2G = (7,14) \quad 9G = (3,11)$$

$$3G = (0,5) \quad 10G = (0,12)$$

$$4G = (3,6) \quad 11G = (7,6)$$

$$5G = (9,14) \quad 12G = (1,10)$$

$$6G = (16,16) \qquad 13G = \mathcal{O}$$

$$7G = (16,1)$$

red podgrupa generirane s G je $n = 13$

$$h = \frac{E(F_{17})}{n} = 1$$

$E(F_{17})$ – predstavlja broj točaka na krivulji.

Nadalje, javni podaci su:

$$y^2 = x^3 + 23x + 42\ mod\ 17,$$
$$G(1,7),$$
$$n = 13$$

Stvaranje ključa:

1. Alice odabire svoj privatni ključ $\alpha = 3$ tako da vrijedi $1 \leq \alpha \leq n - 1$ te računa l po sljedećoj formuli:

$$l = \alpha G = 3G = (0,5)$$

   te rezultat šalje Bobu.

2. Bob odabire svoj privatni ključ β = 7 tako da vrijedi $1 \leq \beta \leq n - 1$ te računa m po sljedećoj formuli:

$$m = \beta G = 7G = (16,1)$$

   te rezultat šalje Alice.

3. Alice računa $\alpha m = 3m = 3(7G) = 21G \ mod \ 17 = 4G = (3,6)$

4. Bob računa $\beta l = 7l = 7(3G) = 21G \ mod \ 17 = 4G = (3,6)$

Vidljivo je kako su Alice i Bob došli do iste točke bez da su pritom odali svoje tajne ključeve.

8. Post-kvantna kriptografija

Pojavom kvantnih računala dolaze vremena kad standardni kriptografski sustavi kao što su RSA, AES, ECC i ostali neće biti dovoljni. Kako bi podaci ostali i dalje sigurni, znanstvenici pokušavaju pronaći nove kriptografske sustave koji će pružati sigurnost protiv kvantnih računala.

8.1 Kvantno računalo

Kvantno računalo je vrsta računala koje koristi kvantno-mehaničke fenomene za izvođenje operacija na podacima. Primjerice, superpoziciju ili kvantnu isprepletenost. Dok klasična računala za predstavljanje podataka koriste bitove koji mogu biti 0 ili 1, kvantna računala upotrebljavaju kvantne bitove ili qbitove. Oni mogu postojati u više stanja istovremeno sve dok se ne mjeri stanje kvantnog bita pri čemu poprimaju vrijednost 0 ili 1.

Kvantni bitovi mogu se interpretirati kao valovi. Jače energetski val može predstavljati 0, a manje energetski val 1, pri čemu svaki kvantni bit ima jednaku vjerojatnost da bude 0 ili 1. Pri radu kvantnog računala više vjerojatnosti kvantnih bitova međusobno

komunicira konstruktivno ili destruktivno baš kao i valovi.
Iako kvantni bitovi mogu postojati u više stanja istovremeno to ne znači da kvantno računalo može izračunati sve „opcije“ nego, kako se algoritam pokreće, tako kvantno računalo vraća više rješenja od kojih je samo jedno točno. Može se reći da kvantno računalo donosi pretpostavku. Zbog toga je potrebno mjeriti i provjeravati rješenja više puta.
Snaga kvantnih računala izražava se u broju kvantnih bitova, što više kvantnih bitova to je kvantno računalo jače.

8.2 Trenutno stanje kvantnih računala

U 2023. godini najbrže kvantno računalo opće namjene jest *Osprey*, kojeg je razvila tvrtka IBM, a sastoji se od 433 kvantna bita [11]. Prema [11], „IBM-ov novi 433-kvantni bitni procesor ima potencijal pokretati složene kvantne izračune koji daleko nadilaze mogućnosti bilo kojeg klasičnog računala. Za referencu, IBM je istaknuo da broj klasičnih bitova koji bi bili potrebni za predstavljanje mogućih stanja na procesoru IBM Osprey daleko premašuje ukupan broj atoma u poznatom svemiru“[3]. Navedeni podaci su veoma impresivni, ali i dalje nedovoljni za razbijanje enkripcije koja se danas koristi.

8.3 Algoritmi za faktorizaciju i rješavanje problema diskretnog logaritma

Protokoli za razmjenu ključeva oslanjaju se na pretpostavku da su određeni matematički problemi preteški da bi se mogli riješiti u razumnom vremenskom roku.
Jedan od takvih problema je već prije spomenuti problem diskretnog logaritma na eliptičkim krivuljama [13]. Njegova je složenost tolika da bi korištenjem trenutnih (klasičnih) algoritama za njegovo rješenje na instanci veličine n bitova trebalo eksponencijalno vrijeme u n, odnosno $2^{n/2}$. U praksi se obično koristi veličina ključa od 256 bitova što znači da najpoznatiji klasični napad na protokol za razmjenu ključeva traje 2^{128} operacija [12].

Jedan od značajnijih algoritama za kvantna računala i enkripciju je Shorov (Shor, 1994)

[3] Preuzeto sa Dashveenjit Kaur, „IBM just unveiled its most powerful quantum computer yet — a 433-qubit machine“

algoritam koji može riješiti problem diskretnog logaritma i problem faktorizacije velikih brojeva u razumnom vremenu.

1. „Prvo se odabire slučajni pozitivni cijeli broj $m < n$, zatim se

najveći zajednički djelitelj (m, n) izračunava u polinomnom vremenu pomoću Euklidovog algoritma. Ako je najveći zajednički djelitelj $(m, n) \neq 1$, prosti faktor od n je pronađen i problem je riješen. Ali, ako je najveći zajednički djelitelj $(m, n) = 1$, prelazi se na korak 2.

2. Korištenjem kvantnog računala dobije se nepoznati period P niza i dan je kako slijedi; $x \; mod \; n, x^2 \; mod \; n, x^3 \; mod \; n, x^4 \; mod \; n$ ...
3. Utvrdi li se da je P neparan cijeli broj, tada se ponavlja prvi korak, a ako je P paran broj, nastavlja se s korakom 4. Za pozitivan period P vrijedi: $\left(m^{\frac{P}{2}} - 1\right)\left(m^{\frac{P}{2}} - 1\right) = m^P - 1 = 0 \; mod \; n$
4. Sljedeći korak je provjeriti je li $m^{P/2} + 1 = 0 \; mod \; n$, i ako da, onda se 1. korak ponavlja. Međutim, ako $m^{P/2} + 1 \neq 0$ prelazi se na korak 5.
5. Konačno, da bi se izračunalo $d = gcd(m^{\frac{P}{2}} - 1, n)$ koristi se Euklidov algoritam, a budući da je $m^{P/2} + 1 \neq 0 \; mod \; n$ dokazan u 4. koraku to pokazuje da je d prosti faktor od n.“ [4]

Shorov algoritam je brži od klasičnih algoritama zbog kvantne Fourierove transformacije koja je eksponencijalno brža od klasične Fourierove transformacije. Trenutna implementacija Shorovog algoritma ograničena je brojem kvantnih bitova koje današnja kvantna računala imaju. Međutim smatra se da će se razvojem novih jačih kvantnih računala te poboljšanjem Shorovog algoritma isti koristiti za razbijanje određenih kriptografskih sustava.

Kao što je već rečeno, kvantna računala predstavljaju veliku prijetnju kriptografskim sustavima koji su danas poznati.

[4] Ovaj opis algoritma je preuzet iz International Journal of Advanced Trends in Computer Science and Engineering, Vol.9, No. 5, 2020, *An overview of Quantum Cryptography and Shor's Algorithm, str. 74-92*

Sljedeća tablica (tablica 3) predstavlja učinak kvantnih računala na poznate kriptografske sustave.

Tablica 3: učinak kvantnih računala na poznate kriptografske sustave

Kriptografski sustav	Vrsta	Svrha	Učinak velikog kvantnog računala
AES	Simetrična	Enkripcija	Treba povećati veličinu ključa
SHA-2, SHA-3		Hashing	Treba povećati izlaz iz funkcije
RSA	Asimetrična	Potpisi, stvaranje ključeva	Nesigurno
ECDSA, ECDH (ECC)	Asimetrična	Potpisi, razmjena ključeva	Nesigurno
DSA	Asimetrična	Potpisi, razmjena ključeva	Nesigurno

Izvor: International Journal of Advanced Trends in Computer Science and Engineering, Vol.9, No. 5, 2020

Iako ova tablica iz NIST-a prikazuje nesigurnost eliptičkih krivulja protiv velikih kvantnih računala, smatralo se da će se eliptičke krivulje i dalje koristiti, ali u obliku izogenija. Smatralo se da će Diffie-Hellmanov protokol za razmjenu ključeva supersingularne izogenije (SIDH) biti siguran protiv kvantnih računala, ali su 5. kolovoza 2022. godine Castryck i Decru objavili kako SIDH i SIKE nisu sigurni za korištenje te da se ne bi smjeli implementirati [16]. Za probijanje ovog protokola bila su dovoljna klasična računala [9].

Otkako se pokazalo da je SIDH nesiguran nema drugih aktivnih kandidata koji se temelje na izogeniji, a koji sudjeluju u NIST standardizaciji [9], [10]. Nakon probijanja SIDH-a smatralo se da je Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) i dalje siguran jer se ne temelji na SIDH-u, ali ne postoji novija dokumentacija koja to potvrđuje ili osporava.

8.4 Izogenija eliptičkih krivulja

Izogenija eliptičke krivulje je posebna vrsta izogenije koja čuva grupnu strukturu eliptičke krivulje. To znači da ako se izogenija eliptičke krivulje primijeni na eliptičku krivulju, rezultirajuća krivulja će imati isti broj točaka u svojoj grupi kao i izvorna krivulja, a grupne operacije na novoj krivulji bit će povezane s onima na izvornoj krivulji na specifičan način.
Drugim riječima, izogenija između dvije krivulje E i E' je karta φ tj. racionalno preslikavanje koje povezuje E i E' tako da svakoj točki P na E dodijeli odgovarajuću točku Q na E' tako da vrijedi $\varphi(P) = Q$ te $\varphi(P + P') = Q + Q'$

Izogenije su važne u kriptografiji jer se mogu koristiti za konstruiranje kriptografskih protokola koji su sigurni protiv određenih vrsta napada.

9. Zaključak

Kriptografija eliptičke krivulje (ECC) postala je sve popularniji kriptografski alat zbog svoje učinkovitosti i sigurnosnih značajki. Međutim, pojavom kvantnog računarstva, sigurnost trenutnih implementacija ECC-a potencijalno može biti ugrožena. Za učinkovito rješavanje problema diskretnog logaritma koji služi kao osnova kriptografije eliptičkih krivulja, kvantna računala koriste Shorov algoritam.
S druge strane, znanstvenici istražuju post-kvantne kriptografske sustave koji se mogu oduprijeti napadima kvantnih računala. Smatralo se da je korištenje izogenija eliptičkih krivulja obećavajući pristup pružanja otpornosti kvantnim napadima budući da se temelje na drugačijem matematičkom problemu. Iako se ispostavilo da je Diffie-Hellmanov protokol za razmjenu ključeva supersingularne izogenije nesiguran, to ne mora nužno značiti kraj za kriptografiju eliptičnih krivulja u post-kvantnom okruženju.

U međuvremenu, važno je da se organizacije koje se oslanjaju na ECC pripremaju za post-kvantnu eru razvojem planova migracije te ulaganjem u istraživanje i razvoj post-kvantne kriptografije. Budući da tehnologija kvantnog računarstva nastavlja napredovati, ključno je biti ispred potencijalnih sigurnosnih prijetnji i osigurati povjerljivost i integritet osjetljivih informacija.

10. Literatura:

[1] - Shevchuk, O. *Introduction to elliptic curve cryptography, 2020.*
Dostupno na: https://math.uchicago.edu/~may/REU2020/REUPapers/Shevchuk.pdf
[2] – Dujella, A. *Eliptičke krivulje u kriptografiji* PMF – MO, Sveučilište u Zagrebu, 2013. Dostupno na: https://web.math.pmf.unizg.hr/~duje/elkript/elkripto2.pdf
[3] - Garry C. Kessler, *An Overview of Cryptography*, 16.4.2015
[4]- Salomaa, A. *Public Key Cryptography*, second edition
Dostupno na: https://books.google.hr/books?hl=en&lr=&id=fgF0WOB_P-4C&oi=fnd&pg=PA1&dq=Salomaa,+A.+Public+Key+Cryptography,+second+edition&ots=0nO2qiDXZN&sig=9bRjrKOZiLHDgwrWIfh1s9SY_pY&redir_esc=y#v=onepage&q=Salomaa%2C%20A.%20Public%20Key%20Cryptography%2C%20second%20edition&f=false
[5] - https://safecurves.cr.yp.to/index.html
[6] - NIST Special Publication NIST SP 800-186 Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters
Eliptic Curve Cryptography An Implementation tutorial
Dostupno na: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-186.pdf
[7] - International Journal of Advanced Trends in Computer Science and Engineering, Vol.9, No. 5, 2020, *An overview of Quantum Cryptography and Shor's Algorithm*
[8]- Wohlwend, J. *ELLIPTIC CURVE CRYPTOGRAPHY: PRE AND POST QUANTUM*
Dostupno na: https://math.mit.edu/~apost/courses/18.204-2016/18.204_Jeremy_Wohlwend_final_paper.pdf
[9] - https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/sike-team-note-insecure.pdf
[10] - Castryck, W, Decru T. *An efficient key recovery attack on SIDH*
Dostupno na:https://eprint.iacr.org/2022/975.pdf
[11] – Dashveenjit Kaur, „IBM just unveiled its most powerful quantum computer yet — a 433-qubit machine", 10. Studenog. 2022,
Dostupno na: https://techhq.com/2022/11/ibm-just-unveiled-its-most-powerful-quantum-computer-yet-a-433-qubit-machine/#:~:text=IBM's%20quantum%20roadmap%20essentially%20consists,its%2

0Kookaburra%20processor%20in%202025
[12] - Grumbling,E. Horowitz, M – *QUANTUM COMPUTING* progress and prospects
[13] - International Journal of Advanced Computer Science and Applications, Vol. 9, No. 3, 2018
[14] - Pratt, K. *Elliptic Curve Cryptography,* 12-18-2014
Dostupno na: https://vc.bridgew.edu/honors_proj/70/
[15]-
https://www.google.com/search?q=ecc+discrete+logarithm+problem&oq=ecc&aqs=chrome.0.69i59j69i57j0i512j69i64j0i512l3j69i65.1143j0j7&sourceid=chrome&ie=UTF-8#fpstate=ive&vld=cid:5ef7634d,vid:eslSF7GrbSw

[16] - Castryck W, Decru T. *An efficient key recovery attack on SIDH*
[17] – Evgeny, M. *The RSA Algorithm* 3 June 2009
Dostupno na: https://pdfdirectory.com/pdf/0702-the-rsa-algorithm.pdf

11. Popis slika

12. Popis Tablica

13. Sažetak

Primarni cilj kriptografije je šifriranje podataka kako bi se isti mogli prenositi putem nesigurnih komunikacijskih kanala. Kriptografija postoji preko 4000 godina te su se vremenom razvijali različiti oblici, ali svi s istim ciljem. Osnovna podjela kriptografije je na simetričnu i asimetičnu kriptografiju. Eliptičke krivulje, temeljni fokus ovog rada, dio su asimetrične enkripcije. One su određene jednadžbom: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ iako se češće koristi kraća Weierstrassova forma: $y^2 = x^3 + ax + b$. Za razumijevanje kriptografije koja koristi eliptičke krivulje važno je znati zbrajanje točaka na eliptičkim krivuljama koje se može podijeliti na zbrajanje točke same sa sobom (eng. *point doubling*) ili zbrajanje dvije različite točke (eng. *point addition*). Kriptografija eliptičkih krivulja temelji se na problemu diskretnog logaritma, odnosno kako pronaći n tako da je $Q = nG$ gdje nG predstavlja dodavanje točke G samoj sebi n puta (*point doubling*).

Napretkom kvantnih računala kriptografija eliptičkih krivulja više neće biti sigurna zbog lakog rješavanja problema diskretnog logaritma. Postoje organizacije koje se bave standardizacijom novih kriptografskih sustava koji bi bili otporni na kvantna računala.

Ključne riječi: kriptografija, eliptičke krivulje, Diffie-Hellman protokol, problem diskretnog logaritma, post-kvantna kriptografija

14. Summary

The primary goal of cryptography is to encrypt data so that it can be transmitted over insecure communication channels. Cryptography has existed for over 4,000 years and different forms have been developed over time, but all with the same goal. Cryptography can be sorted into the following categories: symmetric and asymmetric cryptography. Elliptic curves, which are the main focus of this paper, are part of asymmetric encryption. They are determined by the equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ although the shorter Weierstrass form is more often used: $y^2 = x^3 + ax + b$. To understand cryptography that uses elliptic curves, it is important to know the addition of points on elliptic curves, which can be divided into adding a point to itself (point doubling) or adding two different points (point addition). The cryptography of elliptic curves is based on the discrete logarithm problem, that is, how to find n so that $Q = nG$, where nG represents the addition of point G to itself n times (point doubling).

With the advancement of quantum computers, elliptic curve cryptography will no longer be secure due to the easy solution of the discrete logarithm problem. There are organizations involved in standardizing new cryptographic systems that would be resistant to quantum computers.

Keywords: cryptography, elliptic curves, Diffie-Hellman protocol, discrete logarithm problem, post-quantum cryptography